OPTIMAL LOGIC STRUCTURE OF SAFETY MONITORING SYSTEMS WITH TWO FAILURE MODES(Dissertation_全文)

AUTHOR(S):

Kohda, Takehisa

OPTIMAL LOGIC STRUCTURE OF SAFETY MONITORING SYSTEMS WITH TWO FAILURE MODES

BY

TAKEHISA KOHDA

1983

OPTIMAL LOGIC STRUCTURE OF SAFETY MONITORING SYSTEMS WITH TWO FAILURE MODES

by

Takehisa Kohda

dissertation submitted in partial fulfillment

of the requirements for the degree of

DOCTOR OF ENGINEERING

at

KYOTO UNIVERSITY

Kyoto, JAPAN

1983

ACKNOWLEDGMENTS

The author would like to express his sincere gratitude and appreciation to the following individuals for their aid and encouragement during the completion of this study and the pursuit of his doctorate:

Dr. Hajime Akashi, Professor of Kyoto University, for his continuous encouragement and supervision during the course of this thesis research.

Dr. Koichi Inoue, Associate Professor of Kyoto University, for leading the author into the study of systems reliability and safety, and also for his guidance and valuable discussions.

Dr. Hiromitsu Kumamoto, Research Assistant of Kyoto University, for his excellent suggestions, comments, and discussions.

Dr. Yoichi Ogawara, Mr. Etsuji Sakino, and Mr. Isao Takami, Takasago Technical Institute, Mitsubishi Heavy Industries, Ltd., for their discussions from the practical viewpoint.

Members of Systems Control Laboratory, for their comments and discussions.

Finally, the author wishes to thank his parents, Kinjiro and Sadako, whose understanding and support made the dissertation possible.

T. Kohda

Kyoto JAPAN

March 1983

ABSTRACT

This dissertation develops the optimal logic structure of safety monitoring systems composed of sensors with two kinds of contradictory failures; a failed-dangerous (FD) and a failed-safe (FS) failure. The dissertation is divided into three parts.

The first part considers a safety monitoring system composed of several channels. Each of them consists of identical sensors and supervises a specific plant state, e.g., temperature or pressure. When a state becomes abnormal, the corresponding channel issues a channel alarm and activates protective actions. The problem is to design the optimal coherent structure for each channel, minimizing an expected total loss. For a one-channel safety monitoring system as the simplest case, the optimal structure is proven to be k*-out-of-n:G structure, and a simple formula to obtain k* is also given. Further, we discuss how the optimal k* varies, depending on the FD and FS failure probabilities of the sensor, the failure probability of the plant, and the losses caused by the FD and FS failures of the safety monitoring system. For the multi-channel safety monitoring system, the optimal channel structure is proven to be k-out-of-n:G structure, and the problem is formulated in non-linear integer programming (NLIP). The NLIP problem is then solved by the extended Lawler and Bell's method.

The second part deals with a safety monitoring system composed of various types of sensors. An appropriate protective procedure is activated on the basis of the output of the sensors. The problem is how to obtain the optimal Boolean structure to

combine the sensors, in the sense it minimizes an expected total loss caused by FD and FS failures of the sensors. A simple rule to determine the optimal structure among all the Boolean structures is given by a switching function. Some properties of the switching function is proven for the following three situations: 1) all the sensors monitor the same plant state and their failures are statistically independent, 2) sensors monitor several statistically independent plant states and fail statistically independently, and 3) sensors supervise several statistically dependent plant states. Then, the similar property of the optimal structure for each situation gives a simple systematic search method to determine it and a simple expression of the structure function. A non-coherent structure can be optimal in some case. Analytic solutions are also obtained for the one-plant monitoring safety systems composed of identical sensors.

The last part discusses an optimal shut-down logic for the overall protective system, which is composed of 1) a sensing section, 2) a judging section, and 3) a driving section. The previous two parts consider only FD and FS failures of the sensing section. In this part, each section has two kinds of failures: FD and FS failures. The problem here is to obtain the optimal Boolean shut-down logic that minimizes an expected total loss caused by failures of the overall protective system. The optimal shut-down logic is determined by a simple switching function. A path set expression of the optimal logic is also shown. For an overall protective system with reliable judging and driving sections, the switching function becomes equivalent to

the switching function in the second part; the optimal shut-down logic is determined by the reliability of the sensing section.

CONTENTS

CHAPTER 1

INTRODUCTION

1.1 INTRODUCTION AND HISTORICAL REVIEW

In recent years, such systems as chemical plants, nuclear plants, and electric power supply systems, have shown a rapid trend toward increased size and complexity. Once an accident occurs in these systems, it incurs a great loss of life and property, and further produces environmental disruptions. The losses caused by it are now becoming impossible to estimate. In order to reduce the damage to a minimum, various kinds of protective systems are used. These systems are modeled as shown in Fig. 1.1. In normal operation, the plant is regulated by its control system and its protective system is on standby. When an unlikely emergency or a given type of failure occurs in the plant, or when the control system gets out of order, the protective system must shut down the plant to prevent an accident. The protective system is composed of three sections; sensing, judging, and driving sections. The sensing section is composed of sensors and monitoring the state of the plant. The judging section processes all the signals from the sensing section to decide whether the driving section should be activated or not. The driving section is activated by the command from the sensing section, shutting down the plant. In

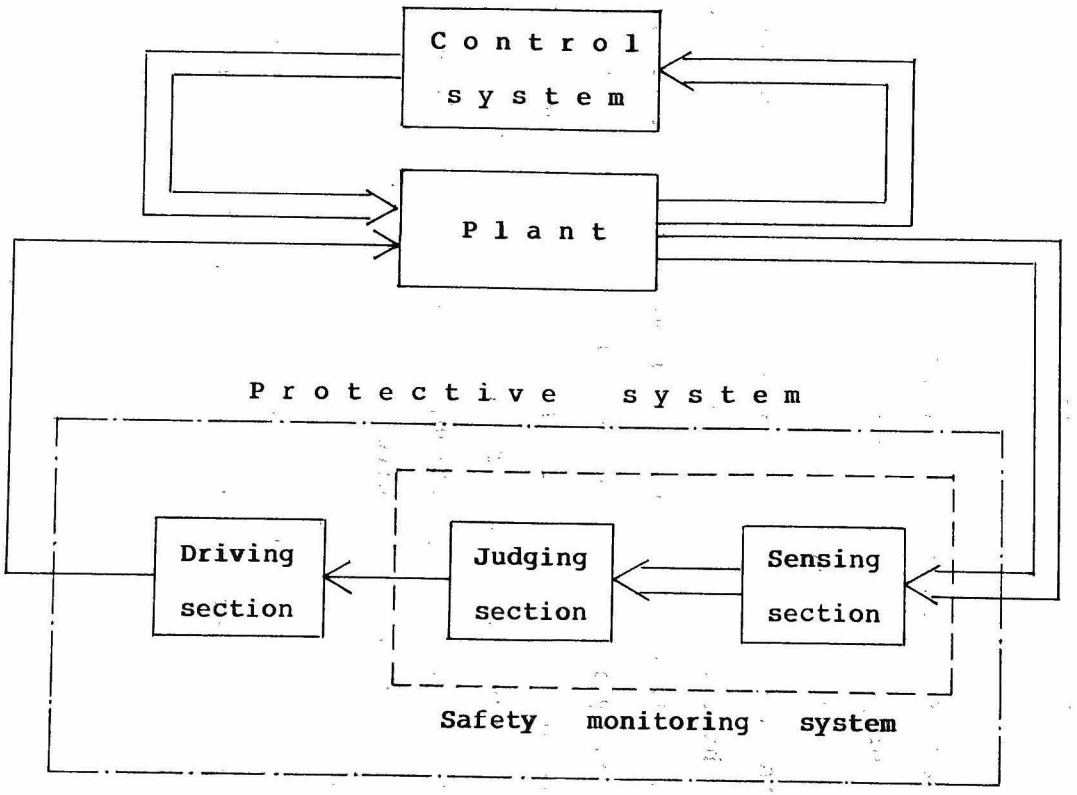

Fig. 1.1 Overall structure of plant combined with protective system

this dissertation, the safety monitoring system is defined as a subsystem of the protective system, which consists of the sensing and judging sections. Thus, the most essential function of the safety monitoring system is to detect premonitory symptoms of an accident as quickly as possible, make an alarm, and activate an appropriate protective procedure. The first requirement is to generate an alarm under an abnormal state of the plant.

Let us consider the case where the plant monitored by the safety monitoring system is normal. The generation of an alarm in this case yields unnecessary protective actions such as a plant shut-down, leading to a reduction in the availability of the system. Spurious alarms are not considered to be harmless from the economical point of view. Further, the frequent occurrence of spurious alarms weakens not only the effectiveness of alarms, but also the function of the safety monitoring systems. For example, in a modern high building two or three thousands of fire detectors are set up, which yield so many spurious alarms as to introduce great confusion into the fire fighting. The second requirement is to issue an alarm only in case of emergency.

According to the above two requirements, sensors used in protective systems, alarm systems, etc., have two kinds of contradictory failures; a failed-dangerous (FD) failure and failed-safe (FS) failure. The former implies that the sensor does not yield its sensor alarm when the state of the plant monitored is abnormal, while the latter implies that the sensor yields the spurious sensor alarm when the plant state is normal. Table 1.1 [S2] shows an example of failure rates of these two failures of a sensor in protective systems. It is interesting to note in Table

Table 1.1 Failed-dangerous rate and Failed-safe rate [S2]

Item	Failed-dangerous rate (faults/year)	Failed-safe rate (spurious faults/year)
Process connection	0.15	0.21
Diff. pressure transmitter	0.14	0.31
Signal line interface	0.007	0.03
Pressure switch	0.03	0.10
Channel wiring and relay to logic	0.02	0.02
Totals	0.347	0.67

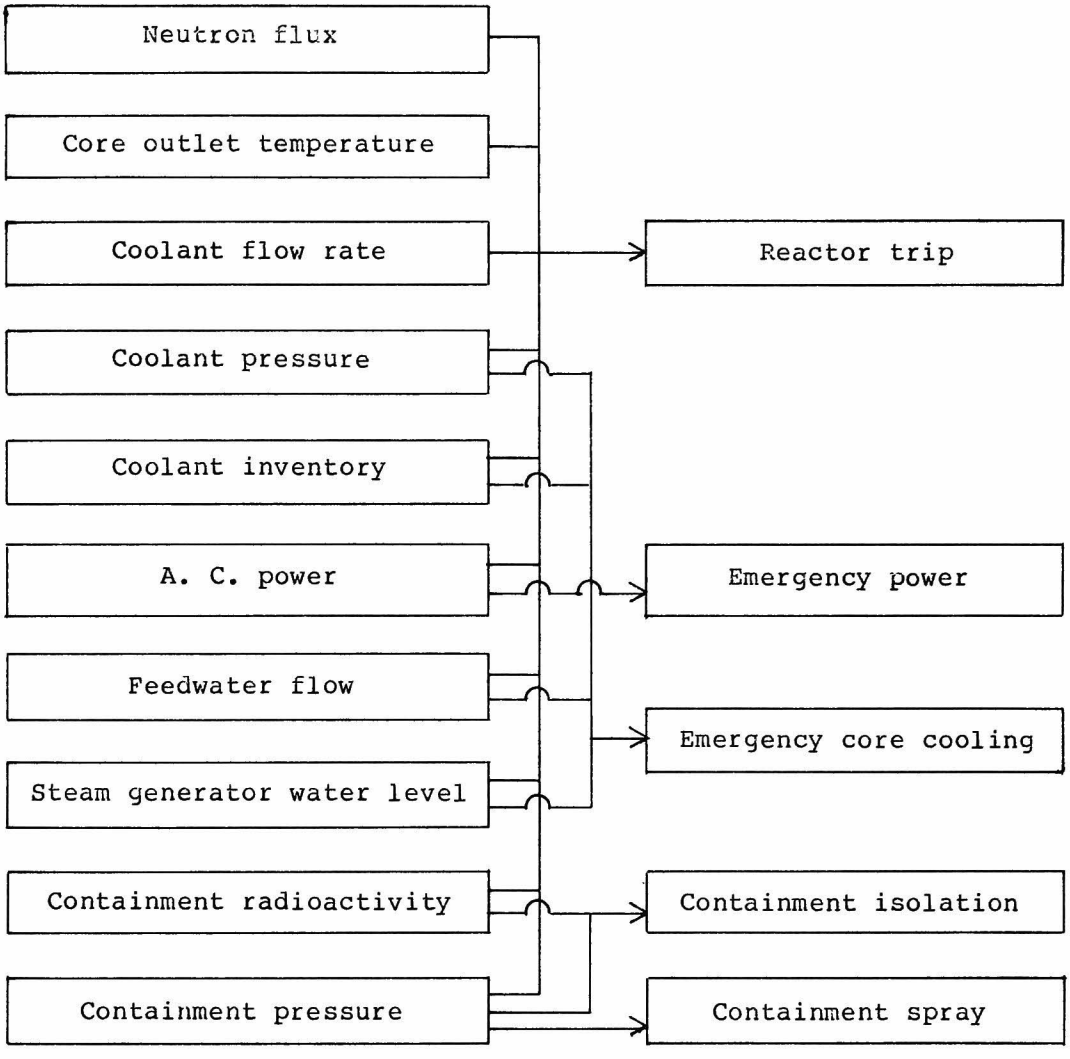

Fig. 1.2 Simplified protective system logic [L2]

1.1 that the FS rate is twice as high as the FD rate. A safety monitoring system composed of a single sensor has limit in its reliability. Thus, in order to obtain a system with higher reliability, safety monitoring systems composed of more than two sensors must be considered and the FS failure must be considered in design as well as the FD failure.

Consider a protective system of a nuclear power plant. Fig. 1.2 [L2] shows a simplified logic diagram to initiate safety systems. There are various events which lead to a plant shut down. In Fig. 1.2, for example, "containment isolation" is activated when the corresponding event, "containment contamination", is detected. This event is defined by an OR combination of abnormal states of the plant; either "containment pressure" or "containment radioactivity" entering an unacceptable range will trip the reactor and cause an appropriate protective procedure, "containment isolation". Thus, different types of sensors which monitor pressure, temperature, flow, flux, level, etc., are applied in these large-scale plants. An orderly protective procedure takes place based on the output of these various types of sensors.

In this dissertation, we consider the optimal logic structure of the safety monitoring system composed of sensors, in the sense it minimizes an expected total loss caused by two kinds of failures of the system.

As typical examples of such a device with two kinds of contradictory failures, there exist fluid flow valves and electric components such as diodes, relays, switches; electric components have "short-circuit" and "open-circuit" failures,

valves are failed in either "stuck-closed" or "stuck-open". The optimal structure design of such a system has been studied in various configurations. These works are summarized in Table 1.2 from the viewpoint of the system configuration. Case 1 analyzed the system composed of identical components and considered the optimal structure in each configuration. Case 2 studied the system composed of several subsystems, each of which consists of identical components. In the lower row of Table 1.2 the system configuration is, the number of structures considered becomes larger. In case 1, the class of coherent structure includes all the other five structures as a part. Kaufmann, Groucho, Cruon [K1] obtained the result that k-out-of-n:G systems are preferable to any other coherent system in case of 3 identical components. More general result was obtained by Phillips [P2]: the k-out-of-n:G systems are preferable to any other coherent system in terms of maximizing the reliability. Further, Ansell, Bendell [A1] recently generalized Phillips' result [P2] to the case where components fail s-dependently. On k-out-of-n:G systems, Ben-Dov [B5] found the optimum k-out-of-n:G system that maximizes the reliability given a fixed number of components. Thus, the optimal structure among coherent systems that maximizes the reliability is analytically obtained by the formula in [B5]. In case 2, both the allocation of components to each subsystem and the determination of subsystem configurations are considered. Kolesar [K10] formulated the problem to minimize one of two failure probabilities in integer linear programming (ILP). Tillman [T3] presented the reliability optimization problems with several failure modes, where these failure modes are classified into two

Table 1.2 Classification I of works on optimal structure design

Case	System configuration	Subsystem configuration	Works
1	Series or parallel	---	[B1], [P3]
	Series-parallel or parallel-series	---	[C2], [G2], [B2], [B3], [K12]
	Hammock networks	---	[M5]
	Two-terminal parallel-series	---	[L3](array), [P1], [N1] [M4]
	k-out-of-n:G	---	[J1], [S3], [M2], [B5]
	Coherent structures	---	[K1], [P2], [A1]
2	Series	Parallel	[K10], [H2]
	Series	Parallel or series	[T3], [H3]
	Series	Series, parallel, parallel-series or series-parallel	[G1]

Table 1.3 Classification II of works on optimal structure design

Optimality criterion	Works
(1) Maximization of the reliability	[M5], [G2], [B1], [P3]. [B2], [B3], [T3], [H2], [H3], [P1], [K1], [G1], [K12], [P2], [B5], [A1]
(2) Maximization of the expected time to failure	[B1], [B2], [B3]
(3) Minimization of one-mode failure probability	[K10]
(4) Minimization of investment cost	[T3], [H2], [H3], [N1]

classes: the class of failure in which the subsystem fails if one component fails, and the class of failure where all the components in the subsystem fail before the subsystem fails. Henin [H2] applied a branch and bound algorithm to a similar problem to [T3]. Hyun [H3] treated [T3] as a 0-1 linear programming (ZOLP) problem and solved it by an implicit enumeration method. Gopal, Aggarwal, Gupta [G1] proposed a heuristic method for [T3]. However, Nakagawa, Hattori [N2] discussed Tillman's treatment [T3] and concluded that [T3], [H3] and [G1] include a common serious error. From the viewpoint of the optimality criterion, these studies are classified as in Table 1.3. Most of the works concentrated on the maximization of the system reliability.

We develop a new optimization problem in the following points compared with the previous studies:

(1) A wider range of system configurations

For the problem of case 1 in the first classification, we first obtain the optimal structure among coherent structures, and further among Boolean structures. In case 2, we do not place a limitation on the system configuration, but we only assume that subsystem structures are coherent at first. Then, we relax this assumption and find the optimal structure among all the Boolean structures. Further, we consider not only the system and subsystems composed of identical components, but also those composed of non-identical components.

(2) A new objective

The objective is to minimize an expected total loss caused by two kinds of contradictory failures of the safety monitoring

system. This objective function expresses the system unreliability as a special case.

Now, we review the studies on protective systems or safety monitoring systems from the viewpoint of the reliability or safety analysis. These studies are roughly divided into two classes: 1) reliability analysis and 2) maintenance or inspection optimization.

1) Reliability analysis:

Kawaguchi, Itō [K2] analyzed reactor instrumentations in view of the reliability, considering various kinds of redundancy. Booth [B7] also considered the effect of variation in redundant tripping logic on the present worth of revenue requirements in electric power generating stations. Nieuwhof [N4] discussed the reliability of "ladder" and "railing" type relay contact arrangements which produce the majority-vote signal in 2-out-of-3:G and 3-out-of-4:G systems. Singh, Patton [S4] described a model of a system and its associated protective system, and then derived suitable relationships for the unreadiness probability and the mean duration of undetected faults. Takami, Inagaki, Sakino, Inoue [T1] considered a problem to allocate fault detectors to find component failures. Kontoleon [K13,K16] analyzed a model of the safeguard with an adequate amount of built-in reliability through the use of redundancy which has a dynamic nature. Kontoleon [K15] presented an overall reliability assessment of an m-out-of-n:G temperature-trip-amplifier system with FD and FS failures. Kontoleon [K17,K18] designed a computer program to analyze the FD and FS probabilities. Kumamoto, Inoue, Henley [K21] developed a computer code which produces time

profiles of expected number of normal trips, spurious trips, and destructive hazards. Kumamoto, Ohtsuka, Inoue [K22] gave formulae to obtain these expected numbers for several systems. Takami, Inoue, Sakino, Kumamoto [T2] dealt with the problem to standby configurations of k-out-of-n:G systems from the viepoint of the cost-effectiveness, considering the FS and FD failures. The effect of failure of majority voters on the reliability of N-tuple modular redundancy systems was analyzed by Mine, Hatayama [M3].

2) Maintenance or inspection optimization:

Kontoleon [K11] studied the availability of a protective system subject to supervisions by a Markov process, considering nothing but FD failures. Chay, Mazumder [C1] considered the problem of determining the test frequency of components of the safeguard, in such a way that an adequate level of readiness is maintained. Kontoleon [K14] analyzed the optimum inspection strategy of an m-out-of-n:G nuclear reactor system with non-identical units, determining both the order and the interval. Inagaki, Inoue, Akashi [I1] dealt with multi-component protective systems with staggered supervision schedules.

On the shut-down logic or configurations of protective systems or safety monitoring systems, most of these studies assumed majority-voting or k-out-of-n:G systems. Little on the preference of these configurations has been analyzed qualitatively and quantitatively.

With advent of digital and linear integrated circuits, not only a higher reliability but also a better system performance can be achieved in the trip logic and shut-off rod drop modules.

The employment of solid state devices throughout the system achieves both a much faster system response and a better reliability. From the practical point of view, several studies have studied on these systems. Ozkaynak [O1] devised a new nuclear safety system through improvements in electrical and/or electronic parts of the system. Harbert [H1] described an automatic protective system which shuts down the plant quickly in a logical sequence following a power failure or a hazard, without damaging the plant. Todd [T4], however, expressed the views about a set of rules constraining the reliability of post-trip cooling systems and the risk of common-mode failures limits the extent to which the microprocessor technology can be employed. Nakamura [N3] introduced a new monitor and alarm system of gas leakage, which uses micro-computers. Kimura, Hasegawa, Sekiguchi [K3] proposed a microprocessor based system for processing redundant instrumentation signals, which has many advantages such as the capacity of performing flexible and complex functions and self-testing features to increase the system reliability. Thus, the trip logic can be selected from a wider range of structures than the conventional majority vote, i.e., k-out-of-n:G systems. We consider all the possible Boolean logic structures in the end to obtain the optimal one, which may be implemented by the use of microprocessors.

1.2 SCOPE OF THE DISSERTATION

The subject of this dissertation is to optimize the logic structure of safety monitoring systems with two kinds of contradictory failures; a failed-dangerous (FD) and a failed-safe

(FS). The main part of the dissertation is divided into three parts. CHAPTER 2 is concerned with the mathematical preliminary. The first part, which consists of CHAPTERS 3 and 4, deals with the optmization of channel structures among coherent structures. The second part consists of CHAPTERS 5, 6, and 7 and is devoted to the optimization of Boolean logic structures to combine sensor signals. The last part, CHAPTER 8, is concerned with the optimal shut-down logic for protective systems which include safety monitoring systems as a part.

CHAPTER 2 presents a mathematical preliminary for the reliability analysis of safety monitoring systems, which will be used in the succeeding developments. Fundamentals of the qualitative and quantitative analyses of safety monitoring systems are given. Typical structures of safety monitoring systems are also introduced.

CHAPTER 3 considers the simplest safety monitoring system that supervises a specific plant state, e.g., temperature or pressure, with n identical sensors. We prove that the optimal coherent structure minimizing an expected total loss is k*-out-of-n:G structure and give a simple formula to find the optimal k*. We also discuss how the optimal k* varies, depending on the FD and FS probabilities of the sensor, the probability of the plant failure and the losses caused by FD and FS failures of the system. One method to obtain the optimal number of sensors is shown in an illustrative example.

CHAPTER 4 is devoted to the optimization of multi-channel safety monitoring systems, where each channel monitors a specific plant state. When some states become abnormal, an "event" occurs.

The channels which monitor these abnormal states then initiate appropriate safety systems. Several different events are assumed. Sensors are either normal or FD or FS. More than one sensors are available for each channel. The problem considered here is to allocate sensors to each channel and to obtain the optimal coherent logic structure for it. The optimal logic structure for each channel is proven to be k-out-of-n:G structure, and then the problem is formulated in non-linear integer programming (NLIP). The NLIP problem is then solved by the extended Lawler and Bell's method.

In CHAPTER 5, we consider the case where a specific plant state is monitored by several kinds of sensors, which are not necessarily identical. The safety monitoring system yields the system alarm based on the output of sensor alarms and activates an appropriate protective procedure. The optimal logic structure that minimizes an expected total loss is obtained by a simple switching function, considering all possible Boolean structures which include non-coherent structures. This is an extension of CHAPTER 3. Several properties of the optimal logic structure are derived; a non-coherent structure can be optimal in some case. We propose a simple systematic search to determine the optimal structure. Analytic solutions are also obtained for systems with identical sensors.

CHAPTER 6 develops the optimal logic structure for the system which supervises several plant states. Each plant state is monitored by several kinds of sensors. The system alarm is generated on the basis of all the sensor alarms. The similar switching function as in CHAPTER 5 gives the optimal Boolean

logic structure. The same development follows.

CHAPTER 7 extends the results of CHAPTERS 5 and 6 into the case where plant states fail statistically dependently. The plant is assumed to suffer losses when any plant state becomes abnormal. We propose a classification of sensors into two classes: "positively reliable" and "negatively reliable". The optimal logic structure is shown to have monotone properties with respect to sensors, depending on the reliability of them. The analytic solutions are also obtained for a system composed of identical sensors.

CHAPTER 8 studies the safety monitoring system combined with safety systems, i.e., the overall protective system. The system considered here is composed of driving, judging, and sensing sections.Each section fails in two ways: FD and FS. The problem is to obtain the optimal shut-down logic that minimizes an expected total loss caused by failures of the system. The optimal shut-down logic is determined by a switching function, which becomes equivalent to the switching function of CHAPTER 6 if the driving and judging sections are reliable.

CHAPTER 9 is a concluding chapter. We summarize the main results obtained in this dissertation, and then states an interesting topic for further research.

CHAPTERS 2 to 8 are partially based on [I2], [I3], [I4], [K4], [K5], [K6], [K7], and [K8].

1.3 PRELIMINARY

$\in$ Basic element of

| Given (given that); used only with operators like

	Pr{ }, E{ }; the condition is on the right; conditional events, per se, are not defined.
$E_a\{\ \}$	Statistically expected value (arithmetic mean, mean, average, first moment); expectation is with respect to the random variable a; the a can be omitted when a is obvious.
Pr{ }	Probability
Pr{ | }	Conditional probability
$\binom{n}{m}$	Number of combinations of n things taken m at a time
s-	implies 'statistical(ly)'
$\coprod_i X_i$	$1 - \prod_i (1-X_i)$
$\underline{\mathbf{Y}} \geq \underline{\mathbf{X}}$	$Y_i \geq X_i$ $(i = 1,\ldots,n)$
$\underline{\mathbf{Y}} > \underline{\mathbf{X}}$	$Y_i \geq X_i$ $(i = 1,\ldots,n)$ with $Y_i > X_i$ for some i

CHAPTER 2

FUNDAMENTALS OF LOGIC STRUCTURE

OF

SAFETY MONITORING SYSTEMS

2.1 INTRODUCTION

The sensor or the safety monitoring system fails in two ways as shown in CHAPTER 1. In the usual reliability analysis, the component or the system is either working or failed. Thus, the usual two-valued analysis cannot be applied to the reliability analysis of the safety monitoring system directly.

In this chapter, we attempt to bring together some of the basic concept of the logic structure of safety monitoring systems. First, the logic structure is modeled by a Boolean function, called "structure function". The concepts of "path" and "cut" are given in the following section. An important class: "coherent structure" is introduced. The FD and FS functions, which show the relationships between the FD and FS failures of the system and those of the sensors, are explicitly expressed in terms of the structure function in section 2.6. The FD and FS probabilities are evaluated by the FD and FS functions, respectively. A "reliability function" is introduced in section 2.7, which plays an important role in calculating the FD and FS

probabilities for the case where sensors fail s-independently. Typical logic structures of safety monitoring systems are introduced in section 2.8, where their FD and FS functions are also shown.

2.2 STRUCTURE FUNCTION OF SAFETY MONITORING SYSTEMS

Assume a safety monitoring system composed of n sensors which are not necessarily identical. Define a binary indicator variable Y_i for sensor i:

$$Y_i = \begin{cases} 1, & \text{if sensor i is generating its sensor alarm,} \\ 0, & \text{otherwise.} \end{cases}$$

Similarly, the safety monitoring system is indicated by a binary indicator variable f as follows.

$$f = \begin{cases} 1, & \text{if the safety monitoring system is generating its system alarm,} \\ 0, & \text{otherwise.} \end{cases}$$

The state of the safety monitoring system is determined completely by the state of the sensors, so that

$$f = f(\underline{Y}), \tag{1}$$

where $\underline{Y} = (Y_1,\ldots,Y_n)$; the n-dimensional vector $\underline{Y}$ specifies an overall state of the n sensors. The function $f(\underline{Y})$ is called an structure function because it tells us how the safety monitoring system generates its system alarm based on the state of the sensors.

The structure function is represented by

$$f(\underline{Y}) = \sum_{\underline{X}} \left[\prod_{i=1}^{n} \{X_iY_i+(1-X_i)(1-Y_i)\} \right] f(\underline{X}), \tag{2}$$

where the sum is extended over all the binary n-dimensional

vector $\underline{X}$.

Given a structure function $f(\underline{Y})$, we define its dual structure function $f^D(\underline{Y})$ by

$$f^D(\underline{Y}) = 1 - f(\underline{1-Y}), \tag{3}$$

where $\underline{1-Y} = (1-Y_1,\ldots,1-Y_n)$.

The concept "dual structure" is useful in analyzing the reliability of systems composed of components subject to two kinds of contradictory failures: FD and FS.

2.3 PATH AND CUT OF SAFETY MONITORING SYSTEMS

Define two exclusive state i and $\bar{i}$ for sensor i.

i : sensor i is generating its sensor alarm.

$\bar{i}$: sensor i is not generating its sensor alarm.

The variable Y_i is the indicator variable for state i. Define by $Y_{\bar{i}}$ an indicator variable for state $\bar{i}$. Then, $Y_{\bar{i}}$ is obviously the complement $\bar{Y}_i$ of Y_i; $\bar{Y}_i = 1-Y_i$.

A path vector is a vector $\underline{Y}$ such that $f(\underline{Y})=1$. The corresponding path set is the set of individual state i or $\bar{i}$ indicated by the vector $\underline{Y}$. A path set ensures the generation of the system alarm. The path set P is minimal if there exists no other path set in P. In other words, the minimal path set P is no longer a path set if some elements are removed from the set P. Assume that the structure function $f(\underline{Y})$ has m minimal path sets $P_1,\ldots,P_m$. The system alarm is generated if and only if some sensors have all the states in at least one minimal path set. Thus,

$$f(\underline{Y}) = \coprod_{k=1}^{m} \left(\prod_{j \in P_k} Y(j) \right) \tag{5}$$

where

$$Y(j) = \begin{cases} Y_i, & \text{if } j=i, \\ \bar{Y}_i, & \text{if } j=\bar{i}. \end{cases} \tag{6}$$

This expression is called a minimal path representation of the structure function. The second product term takes on the unity value if and only if all the states in set P_k occur simultaneously.

A cut vector is a vector $\underline{Y}$ such that $f(\underline{Y})=0$. The corresponding cut set is the set of individual sensor state i or $\bar{i}$ in $\underline{Y}$. A cut set ensures the non-existence of the system alarm. The cut set K is minimal if there exists no other cut set in K. In other words, the minimal cut set K is no longer a cut set if some elements are removed from K. Assume that the structure function $f(\underline{Y})$ has s minimal cut sets $K_1, \ldots, K_s$. The system alarm is not generated as long as some sensors create all the states in at least one minimal cut set. Thus, the structure function $f(\underline{Y})$ is expressed as:

$$f(\underline{Y}) = \prod_{k=1}^{s} \left(\coprod_{j \in K_k} \bar{Y}(j) \right) \tag{7}$$

This is called a minimal cut representation of the structure function. The second union takes on the unity value if and only if some state in set K_k does not occur.

Clearly from the definition of the dual structure function: eq. (3), if $\underline{Y}$ is a path vector for $f(\underline{Y})$, then $\underline{1-Y}$ is a cut vector for $f^D(\underline{Y})$, and vice versa. A set of complement states for a minimal path set P_j of $f(\underline{Y})$ is a minimal cut set for $f^D(\underline{Y})$

and vice versa.

A path set and a cut set are called an "implicant" and an "implicate", respectively in the Boolean algebra, while the minimal path set and the minimal cut set are termed as "prime implicant" and "prime implicate".

2.4 COHERENT STRUCTURE

We now introduce the "coherence" [B4,B6] of the safety monitoring system.

The structure function is coherent if and only if the following two conditions are satisfied:

(1) Monotone Property:

The structure function is monotone increasing; if $\underline{Y} \leq \underline{Y}'$, then $f(\underline{Y}) \leq f(\underline{Y}')$.

(2) Relevance:

For any sensor i, there exists a state $\underline{Y}(i)=(Y_1,\ldots,Y_{i-1},Y_{i+1},\ldots,Y_n)$ such that

$$f(0_i:\underline{Y}(i))=0,$$

and

$$f(1_i:\underline{Y}(i))=1,$$

where $(a_i:\underline{Y}(i)) = (Y_1,\ldots,Y_{i-1},a,Y_{i+1},\ldots,Y_n)$.

NOTE: The i-th sensor is irrelevant to the structure function if $f(\underline{Y})$ is constant in Y_i, that is , $f(1_i:\underline{Y}(i))=f(0_i:\underline{Y}(i))$ for all $\underline{Y}(i)$. Otherwise, the i-th sensor is relevant to the structure function.

The causality is derived from these two conditions:

$$f(\underline{Y}=(0,\ldots,0)) = 0, \tag{8}$$

$$f(\underline{Y}=(1,\ldots,1)) = 1. \tag{9}$$

We can remove irrelevant indicator variables from the arguments of $f(\underline{Y})$. Thus, the relevance can be restored if some variables are relevant. The monotone property is the most essential requirement for the coherent structure function.

The monotone increasing function has a simple structure.

(A) A minimal path vector $\underline{Y}$ is a path vector such that $\underline{Y}'<\underline{Y}$ implies $f(\underline{Y}')=0$. The corresponding minimal path set is $C_1(\underline{Y})=\{i|Y_i=1\}$. Physically, a minimal path set is a minimal set of sensor state i which ensures the generation of the system alarm.

(B) A minimal cut vector $\underline{Y}$ is a cut vector such that $\underline{Y}<\underline{Y}'$ implies $f(\underline{Y}')=1$. The corresponding cut set is $C_0(\underline{Y})=\{\bar{i}|Y_0=0\}$. A minimal cut set is a minimal set of sensor state $\bar{i}$ which prevents the generation of the system alarm.

2.5 FD AND FS FUNCTIONS

The combinations of the state of the safety monitoring system and the state of the plant are:

1) $f(\underline{Y})=1$ and $X=1$,

2) $f(\underline{Y})=1$ and $X=0$,

3) $f(\underline{Y})=0$ and $X=1$,

4) $f(\underline{Y})=0$ and $X=0$,

where X is a binary indicator variable for the state of the plant:

$$X = \begin{cases} 1, & \text{if the plant to be monitored is abnormal,} \\ 0, & \text{otherwise.} \end{cases}$$

States 1) and 4) are the normal states of the safety monitoring system. State 2) is a FS state and state 3) is a FD state of the

safety monitoring system. The failures in states 2) and 3) are respectively called a FS failure and a FD failure of the safety monitoring system.

Similarly, four combinations of the state of the i-th sensor and the state of the plant are:

1') Y_i=1 and X=1,

2') Y_i=1 and X=0,

3') Y_i=0 and X=1,

4') Y_i=0 and X=0.

States 1') and 4') are the normal states of the i-th sensor. State 2') is a FS state and state 3') is a FD state of the i-th sensor. The failures in states 2') and 3') are called a FS failure and a FD failure of the i-th sensor, respectively.

As shown above, the failures of the safety monitoring system and the sensor can be defined only if the environment monitored by them is specified. A sensor is not failed if it does not generate the sensor alarm under the normal state of the plant, while it is failed if it does not under the abnormal state.

Now we obtain the relationship between failures of the sensors and those of the safety monitoring system. Consider the FS failure first.

Assume that the safety monitoring system is placed in a safe environment. The sensor state $\underline{Y}$ is now conditioned by the safe environment. Define the FS function f_{FS} of the safety monitoring system:

$$f_{FS}(\underline{Y}) = \begin{cases} 1, & \text{if the safety monitoring system is FS,} \\ 0, & \text{otherwise,} \end{cases}$$

where

$$Y_i = \begin{cases} 1, & \text{if sensor } i \text{ is generating its sensor alarm under} \\ & \text{the safe environment, i.e., the } i\text{-th sensor is FS,} \\ 0, & \text{otherwise under the safe environment.} \end{cases}$$

The FS function obviously coincides with the structure function $f(\underline{Y})$ where state vector $\underline{Y}$ is now conditioned by the safe environment:

$$f_{FS}(\underline{Y}) = f(\underline{Y}). \tag{10}$$

Assume that the safety monitoring system is placed in an unsafe environment. The sensor state $\underline{Y}$ is now conditioned by the unsafe environment. The variable $\bar{Y}_i = 1 - Y_i$, the complement of Y_i, tells whether sensor i is FD or not:

$$\bar{Y}_i = \begin{cases} 1, & \text{if sensor } i \text{ is not generating its sensor alarm under} \\ & \text{the unsafe environment, i.e., the } i\text{-th sensor is FD,} \\ 0, & \text{otherwise under the unsafe environment.} \end{cases}$$

The FD function of $\underline{\bar{Y}} = (\bar{Y}_1, \ldots, \bar{Y}_n)$ is defined by

$$f_{FD}(\underline{\bar{Y}}) = \begin{cases} 1, & \text{if the safety monitoring system is FD,} \\ 0, & \text{otherwise.} \end{cases}$$

The safety monitoring system is FD if and only if it fails to generate the system alarm under the unsafe environment: $f_{FD}(\underline{\bar{Y}})=1$ is equivalent to $f(\underline{Y})=0$, where $\underline{\bar{Y}} = \underline{\mathbf{1}-\mathbf{Y}}$. Therefore

$$f_{FD}(\underline{\bar{Y}}) = 1 - f(\underline{\mathbf{1}-\bar{\mathbf{Y}}}). \tag{11}$$

Note that the FD function $f_{FD}(\underline{\bar{Y}})$ is the dual of $f(\underline{\bar{Y}})$.

2.6 FD AND FS PROBABILITIES

In this section we give expressions of FD and FS probabilities of the safety monitoring system. They can be calculated, given the structure function $f(\underline{Y})$.

First, we define FD and FS probabilities of the sensor. Assume that the sensor i monitors the plant. Sensor i is FS if and only if it generates the sensor alarm under the normal state of the plant. Thus, the conditional FS probability q_{2i} of sensor i is:

$$q_{2i} = \Pr\{Y_i=1 \mid X=0\}. \tag{12}$$

Sensor i is FD if and only if it fails to generate the sensor alarm under the abnormal state of the plant. The conditional FD probability q_{1i} of the sensor i is:

$$q_{1i} = \Pr\{Y_i=0 \mid X=1\}. \tag{13}$$

The safety monitoring system is FS if and only if it generates the system alarm under the normal plant state. Thus, the conditional FS probability Q_{2S} is:

$$\begin{aligned} Q_{2S} &= \Pr\{f_{FS}(\underline{Y})=1 \mid X=0\} \\ &= E\{f_{FS}(\underline{Y}) \mid X=0\}. \end{aligned} \tag{14}$$

Eq. (10): $f_{FS}(\underline{Y})=f(\underline{Y})$ yields the expression in terms of the structure function $f(\underline{Y})$:

$$\begin{aligned} Q_{2S} &= E\{f(\underline{Y}) \mid X=0\} \\ &= \sum_{\underline{Y}} f(\underline{Y}) \Pr\{\underline{Y} \mid X=0\}. \end{aligned} \tag{15}$$

The conditional FS probability is the expected value of the structure function under the safe environment.

The safety monitoring system is FD if and only if it fails to generate the system alarm under the abnormal state of the plant. The conditional FD probability Q_{1S} is

$$Q_{1S} = E\{f_{FD}(\underline{\bar{Y}}) \mid X=1\}. \tag{16}$$

Eq. (11) yields the expression of Q_{1S} in terms of the structure function $f(\underline{\bar{Y}})$:

$$Q_{1S} = E\{1-f(\underline{\mathbf{1}-\bar{Y}}) \mid X=1\}$$

$$= 1 - \sum_{\underline{Y}} f(\underline{Y}) \Pr\{\underline{Y} | X=1\}. \tag{17}$$

2.7 RELIABILITY FUNCTION

Let $h(\underline{Y})$ be a sum of product (S.O.P) expression of the structure function $f(\underline{Y})$. Two methods are typically used to obtain $h(\underline{Y})$:

(1) Truth Table Approach

The function $h(\underline{Y})$ is obtained by picking up from the table the exclusive combinations of the sensor state $\underline{Y}$ such that $f(\underline{Y})=1$.

$$h(\underline{Y}) = \sum_{\underline{U}} f(\underline{U}) \left[\prod_{i=1}^{n} \{Y_i U_i + (1-Y_i)(1-U_i)\} \right]. \tag{18}$$

This expression is a canonical form of $f(\underline{Y})$.

(2) Expansion Approach

The function $h(\underline{Y})$ is obtained by expanding the minimal path representation or the minimal cut representation or any form of $f(\underline{Y})$, with the simplification rule: $Y_i^2 = Y_i$.

The function $h(\underline{Y})$ is called "reliability function" because it can express various reliability parameters on the system level in terms of the reliability parameters on the component level.

If the sensors fail s-independently, the probabilities Q_{1S} and Q_{2S} can be calculated in terms of the reliability function $h(\mathbf{Y})$ as follows:

$$Q_{1S} = 1 - h(\underline{\mathbf{1}-\mathbf{q}}_1), \tag{19}$$

$$Q_{2S} = h(\underline{\mathbf{q}}_2), \tag{20}$$

where $\underline{\mathbf{1}-\mathbf{q}}_1 = (1-q_{11},\ldots,1-q_{1n})$ and $\underline{\mathbf{q}}_2 = (q_{21},\ldots,q_{2n})$.

2.8 TYPICAL STRUCTURE OF SAFETY MONITORING SYSTEMS

In this section, we introduce typical structures of the safety monitoring systems: "series structure", "parallel structure", "k-out-of-n:G structure", and "k-out-of-n:F structure".

1) Series Structure

A series structure generates its system alarm if and only if each sensor generates its sensor alarm. The structure function is given by

$$f(\underline{Y}) = \prod_{i=1}^{n} Y_i. \tag{21}$$

2) Parallel Structure

A parallel structure generates its system alarm if and only if at least one sensor generates its sensor alarm. The structure function is given by

$$f(\underline{Y}) = \coprod_{i=1}^{n} Y_i. \tag{22}$$

3) k-out-of-n:G Structure

A k-out-of-n:G structure generates its system alarm if and only if k or more of its n sensors generate sensor alarms. The structure function is given by

$$f(\underline{Y}) = \begin{cases} 1, & \text{if } S(\underline{Y}) \geq k, \\ 0, & \text{if } S(\underline{Y}) < k, \end{cases} \tag{23}$$

where $S(\underline{Y}) = \sum_{i=1}^{n} Y_i$.

Note that a series structure is an n-out-of-n:G structure, and a parallel structure is a 1-out-of-n:G structure.

4) k-out-of-n:F Structure

A k-out-of-n:F structure generates the system alarm if and only if k or more of its n sensors do not generate sensor alarms. The structure function is given by

$$f(\underline{Y}) = \begin{cases} 1, & \text{if } S(\underline{Y}) \leq n-k, \\ 0, & \text{if } S(\underline{Y}) > n-k. \end{cases} \tag{24}$$

Obviously, this structure is non-coherent because it does not satisfy the monotone increasing property. On the other hand, the previous three structures are coherent.

For a series or parallel structure, the reliability function coincides with the expression of the structure function: eq. (21) or (22). The k-out-of-n:G and k-out-of-n:F structures have the following reliability functions, assuming that all the sensors are identical.

k-out-of-n:G structure:

$$h(\underline{Y}) = \sum_{i=k}^{n} \binom{n}{i} Y^i (1-Y)^{n-i}, \tag{25}$$

k-out-of-n:F structure:

$$h(\underline{Y}) = \sum_{i=k}^{n} \binom{n}{i} (1-Y)^i Y^{n-i}. \tag{26}$$

Lastly, we introduce two typical non-coherent structures; one is a safety monitoring system with continuous alarm and the other is a safety monitoring system without alarm. The structure function of continuous alarm is:

$$f_C(\underline{Y}) = 1, \quad \text{for all } \underline{Y}. \tag{27}$$

There is only one minimal path set which is empty; the system alarm is generated all the time irrespective of the sensor states. This system is not failed-dangerous, while it is always failed-safe. The system without alarm has the following structure

function:

$$f_N(\underline{Y}) = 0, \quad \text{for all } \underline{Y}. \tag{28}$$

There is no path set since the system alarm is never generated. The system is always failed-dangerous, while it is never failed-safe. The continuous-alarm system is considered to be a 0-out-of-n:G or a 0-out-of-n:F structure and the no-alarm system is considered to be an (n+1)-out-of-n:G or an (n+1)-out-of-n:F structure.

Table 2.1 shows FD and FS functions for the systems described in this section, where all the sensors are identical.

Table 2.1 FD and FS functions of safety monitoring systems

	FD function	FS function
Series	$1 - (1-\bar{Y})^n$	Y^n
Parallel	$\bar{Y}^n$	$1 - (1-Y)^n$
k-out-of-n:G	$\sum_{i=k}^{n} \binom{n}{i} (1-\bar{Y})^i \bar{Y}^{n-i}$	$\sum_{i=k}^{n} \binom{n}{i} Y^i (1-Y)^{n-i}$
k-out-of-n:F	$\sum_{i=k}^{n} \binom{n}{i} \bar{Y}^i (1-\bar{Y})^{n-i}$	$\sum_{i=k}^{n} \binom{n}{i} (1-Y)^i Y^{n-i}$
Continuous-Alarm	0	1
No-Alarm	1	0

CHAPTER 3

OPTIMAL COHERENT STRUCTURE

OF

ONE-CHANNEL SAFETY MONITORING SYSTEMS

3.1 INTRODUCTION

The safety monitoring system composed of identical sensors is considered as the simplest case. All the sensors supervise the same state of the plant, e.g., temperature or pressure. Through CHAPTERS 3 and 4, a channel means a group of these identical sensors, monitoring a specific state of the plant. Thus, the safety monitoring system considered here is called "one-channel". while we deal with "multi-channel" systems in the next chapter.

The optimal logic structure that minimizes an expected total loss caused by FD and FS failures of the system is analytically obtained among all the coherent structures composed of n identical sensors. A simple formula is given in section 3.3.1 to find the optimal structure. We discuss how the optimal structure changes, depending on the FS and FD probabilities of the sensor, the probability of the plant failure, and the losses caused by the FD and FS failures of the safety monitoring system in the following section. The number of sensors used for the system is also optimized in an illustrative example.

3.2 PROBLEM STATEMENT

3.2.1 Assumptions

1 The safety monitoring system is composed of one channel, which consists of n identical sensors.

2 The safety monitoring system supervises a specific state of the plant.

3 The safety monitoring system is coherent.

4 Sensors fail s-independently.

5 Sensors are reliable: $q_{1i} + q_{2i} < 1$.

3.2.2 Notation

q_1, q_{1i}	conditional FD probability of a sensor
q_2, q_{2i}	conditional FS probability of a sensor
$\underline{1-q_1}$	$(1-q_{11},\ldots,1-q_{1n})$
$\underline{q_2}$	$(q_{21},\ldots,q_{2n})$
Q_{1S}	conditional FD probability of the safety monitoring system
Q_{2S}	conditional FS probability of the safety monitoring system
C_{1S}	FD loss: loss caused when the safety monitoring system fails to generate the system alarm, the plant state being abnormal.
C_{2S}	FS loss: loss caused when the safety monitoring system generates the system alarm, the plant being normal.
I_S	s-expected total loss caused by failures of the safety monitoring system
P	probability that the plant state is abnormal.

$h(\underline{Y})$ reliability function of the safety monitoring system.

INT[k] minimum integer that is larger than or equal to k; for a positive integer k, INT[k] can be either k or k+1.

From assumptions 1 and 4, conditional probabilities Q_{1S} and Q_{2S} are:

$$Q_{1S} = 1 - h(\underline{1-q_1}), \tag{1}$$

$$Q_{2S} = h(\underline{q_2}). \tag{2}$$

The problem is to obtain the optimal coherent structure that minimizes an s-expected total loss caused by failures of the safety monitoring system.

3.3 PROBLEM SOLUTION

3.3.1 Optimal Coherent Structure

The plant suffers losses both when the safety monitoring system fails to function under the abnormal state of the plant, and when the safety monitoring system generates the system alarm with the plant being normal. Then, the s-expected total loss I_S is:

$$I_S = C_{1S}PQ_{1S} + C_{2S}(1-P)Q_{2S}. \tag{3}$$

Whatever values C_{1S}, C_{2S}, and P may take on, the k*-out-of-n:G structure is proven to be optimal among all the coherent structures composed of n identical sensors. Furthermore the optimal k* is found by the following simple formula.

THEOREM :

Let q_1 be the FD probability and let q_2 be the FS probability of the sensor. Assume n sensors. The k*-out-of-n:G structure is optimal in the sense that it minimizes I_S among all

the coherent structures composed of n identical sensors. The values of k* is:

1) $k^* = n$, if $C_{1S}P(1-q_1)^n \leq C_{2S}(1-P)q_2^n$.

2) $k^* = 1$, if $C_{1S}P(1-q_1)q_1^{n-1} \geq C_{2S}(1-P)q_2(1-q_2)^{n-1}$,

3) $k^* = INT[k]$, otherwise,

where

$$k = \frac{\ln\frac{C_{2S}(1-P)}{C_{1S}P} + n \ln\frac{1-q_2}{q_1}}{\ln\frac{(1-q_1)(1-q_2)}{q_1 q_2}}. \qquad (4)$$

Proof :

The reliability function $h(\underline{Y})$ of a coherent structure of n identical sensors is

$$h(\underline{Y}) = \sum_{i=0}^{n} A_i Y^i (1-Y)^{n-i}, \qquad (5)$$

where A_i: the number of ways we can select $i(\leq n)$ sensors such that if these are generating the sensor alarms and the remaining are not generating the sensor alarms, then the safety monitoring system is yielding the system alarm. The causality of the coherentstructure (see section 2.4 of CHAPTER 2) shows that $A_0=0$ and $A_n=1$. From the definition of A_i,

$$0 \leq A_i \leq \binom{n}{i}. \qquad (6)$$

From eqs. (1), (2), (5) and assumption 4, the s-expected total loss I_S is

$$I_S = C_{1S}P - \sum_{i=1}^{n} A_i \{ C_{1S}P(1-q_1)^i q_1^{n-i} - C_{2S}(1-P)q_2^i(1-q_2)^{n-i} \}. \qquad (7)$$

From assumption 5, we may easily see:

1) If $C_{1S}P(1-q_1)^n \leq C_{2S}(1-P)q_2^n$, then

$C_{1S}P(1-q_1)^i q_1^{n-i} - C_{2S}(1-P)q_2^i(1-q_2)^{n-i} < 0$, for $i < n$.

2) If $C_{1S}P(1-q_1)q_1^{n-i} \geq C_{2S}(1-P)q_2(1-q_2)^{n-i}$, then
$C_{1S}P(1-q_1)^i q_1^{n-i} - C_{2S}(1-P)q_2^i(1-q_2)^{n-i} \geq 0$, for $i > 1$.

3) Otherwise, there exists k such that $C_{1S}P(1-q_1)^k q_1^{n-k} = C_{2S}(1-P)q_2^k(1-q_2)^{n-k}$ and if $i \geq k$, then
$C_{1S}P(1-q_1)^i q_1^{n-i} - C_{2S}(1-P)q_2^i(1-q_2)^{n-i} \geq 0$.

Consequently, the following inequality holds;

$$I_S \geq C_{1S}P - \sum_{i=k^*}^{n} A_i\{ C_{1S}P(1-q_1)^i q_1^{n-i} - C_{2S}(1-P)q_2^i(1-q_2)^{n-i} \}, \quad (8)$$

where k^* is determined as the theorem. The equality in eq. (8) holds if and only if $A_i = 0$. for all $i < k^*$.

Further, from eq. (6),

{Right hand side of eq. (8)}

$$\geq C_{1S}P - \sum_{i=k^*}^{n} \binom{n}{i}\{C_{1S}P(1-q_1)^i q_1^{n-i} - C_{2S}(1-P)q_2^i(1-q_2)^{n-i}\}. \quad (9)$$

The equality in eq. (9) holds if and only if $A_i = \binom{n}{i}$, for all $i \geq k^*$. The right hand side of eq. (9) is the minimum of I_S.

Thus, the s-expected total loss I_S takes the minimum if and only if $A_i = 0$, for $i < k^*$, and $A_i = \binom{n}{i}$, for $i \geq k^*$. In this case, the optimal reliability function $h^*(\underline{Y})$ is:

$$h^*(\underline{Y}) = \sum_{i=k^*}^{n} \binom{n}{i} Y^i (1-Y)^{n-i}.$$

This is the reliability function of the k*-out-of-n:G structure (see eq. (25) in section 2.8 of CHAPTER 2).

Q.E.D.

For a special case where $C_{1S} = C_{2S}$ and $P = 0.5$, Ben-Dov [B5] obtained the same result.

Reliability R_S of the safety monitoring system with two kinds of failures is defined by

$$R_S = 1 - PQ_{1S} - (1-P)Q_{2S}. \tag{10}$$

This is the probability of the normal operation of the safety monitoring system. The optimal structure that minimizes R_S is obtained by the theorem with $C_{1S} = C_{2S} = 1$.

3.3.2 Properties of Optimal Coherent Structure

We now discuss how the optimal k* varies, depending on q_1, q_2, P or C_{1S}/C_{2S} in this section.

By differentiating k (eq. (4)) with respect to each of the variables, we have

$$\frac{\partial k}{\partial q_1} = \left(\frac{k}{1-q_1} - \frac{n-k}{q_1} \right) / \ln \frac{(1-q_1)(1-q_2)}{q_1 q_2}, \tag{11}$$

$$\frac{\partial k}{\partial q_2} = \left(\frac{k}{q_2} - \frac{n-k}{1-q_2} \right) / \ln \frac{(1-q_1)(1-q_2)}{q_1 q_2}, \tag{12}$$

$$\frac{\partial k}{\partial P} = - \frac{1}{P(1-P)} / \ln \frac{(1-q_1)(1-q_2)}{q_1 q_2}, \tag{13}$$

$$\frac{\partial k}{\partial \left(\frac{C_{1S}}{C_{2S}}\right)} = - \frac{C_{2S}}{C_{1S}} / \ln \frac{(1-q_1)(1-q_2)}{q_1 q_2}. \tag{14}$$

Since $0 < P < 1$ and $q_1 + q_2 < 1$ in eq. (13), $\partial k / \partial P < 0$. Similarly, $\partial k / \partial (C_{1S}/C_{2S}) < 0$. Therefore, the optimal k* has the following properties.

1) k* gets closer to 1 as the demand probability P gets larger.

2) k* gets closer to 1 as the FD loss C_{1S} gets larger.

3) k* gets closer to 1 as the FS loss C_{2S} gets smaller.

These trends are consistent with the property of k-out-of-n:G

structures that the FD probability becomes lower and the FS probability becomes higher as k gets closer to 1. Such monotone trends do not hold for the FD and FS probabilities of the sensor. Counter examples exist (see EXAMPLE 3 in section 3.4).

3.4 ILLUSTRATIVE EXAMPLE

EXAMPLE 1 :

Values of C_{1S}, C_{2S}, q_1, and q_2 are:

$C_{1S} = 1x10^4$, $C_{2S} = 1x10^2$ $P = 0.1$,

$q_1 = 0.05$, $q_2 = 0.10$.

Table 3.1 shows the optimal structure where n ranges from 2 to 5.

Table 3.1 Optimal structures of EXAMPLE 1

n	Optimal structure	Expected total loss
2	1-out-of-2:G	19.600
3	2-out-of-3:G	9.770
4	2-out-of-4:G	5.188
5	3-out-of-5:G	1.928

As shown in Table 3.1, the s-expected total loss becomes smaller as the number of available sensors gets larger. The theorem shows this property, because the reliability function h(**Y**), eq. (5), can express all the possible coherent structures composed of at most n sensors.

EXAMPLE 2 :

The s-expected total loss becomes smaller as the number of sensors gets larger as shown in EXAMPLE 1. On the other hand the investment cost of the safety monitoring system becomes higher. From the economical point of view, this cost must be balanced with the s-expeted total loss. The minimization of objective function I_S':

$$I_S' = C_{1S}PQ_{1S} + C_{2S}(1-P)Q_{2S} + C(n),$$

where C(n): investment cost function of the safety monitoring system; it is monotone increasing with respect to n,

is now investigated. For a given n, the optimal structure that minimizes $I_S = C_{1S}PQ_{1S} + C_{2S}(1-P)Q_{2S}$ is analytically obtained by the theorem. So the optimal structure is easily found by searching the optimal number of sensors, n*, that minimizes I_S'. In this example, let $C(n) = c_s n$, where c_s is the cost of a sensor. Suppose that values of C_{1S}, C_{2S}, P, c_s, q_1, and q_2 are:

$C_{1S} = 1x10^4$, $C_{1S} = 1x10^2$, $P = 0.1$,

$c_s = 10$, $q_1 = 0.05$, $q_2 = 0.15$.

Table 3.2 shows the searching process to obtain n*. The optimal structure is 2-out-of-3:G structure with $I_S' = 42.717$.

Table 3.2 Searching process of EXAMPLE 2

n	Optimal structure	I_S	I_S'
1	1-out-of-1:G	63.500	73.500
2	1-out-of-1:G	27.475	47.475
3	2-out-of-3:G	12.717	42.717*
4	2-out-of-4:G	10.338	50.338
5	3-out-of-5:G	3.553	53.553

*: Optimal structure of EXAMPLE 2

EXAMPLE 3 :

From eqs. (11) and (12), whether k* gets closer to 1 or not as the FD or FS failure probability of the sensor gets larger depends on values of the FD loss, the FS loss, the failure probability of the plant, and the number of sensors. We give a counter example to show that the monotone trend does not hold for the FD or FS probability of the sensor.

Suppose that values of C_{1S}, C_{2S}, P, q_1, and n are:

$C_{1S} = 1 \times 10^4$, $C_{2S} = 1 \times 10^2$, P = 0.1,

$q_1 = 0.05$, n = 5.

Consider the optimal structure for the following three different values of the FS probability of the sensor: q_2.

Case 1: $q_2 = 0.4$, Case 2: $q_2 = 0.6$, Case 3: $q_2 = 0.8$.

The results are shown in Table 3.3.

Table 3.3 Optimal structure of EXAMPLE 3

	Optimal structure	Expected total loss
Case 1	3-out-of-5:G	29.728
Case 2	4-out-of-5:G	52.919
Case 3	3-out-of-5:G	85.945

We observe that the value of k* does not always get closer to 1 as q_2 gets smaller. A similar counter example exists for q_1, the FD probability of the sensor. However, if q_1 and q_2 are sufficiently small compared with 1/n, then eqs. (11) and (12) show that $\partial k/\partial q_1 < 0$ and $\partial k/\partial q_2 > 0$, respectively. In this case, the optimal k* gets closer to 1 as q_1 gets higher, while the optimal k* gets closer to n as q_2 gets higher.

CHAPTER 4

OPTIMAL COHERENT STRUCTURE

OF

MULTI-CHANNEL SAFETY MONITORING SYSTEMS

4.1 INTRODUCTION

As shown in Fig. 1.2 of CHAPTER 1, the large-scale safety monitoring system involves different types of sensors which monitor pressure, temperature, flow, flux, etc. An orderly shut-down procedure takes place based on the output of these channels. Thus, we develop an optimal structure of multi-channel safety monitoring systems, where channels of different types are logically connected to initiate safety systems.

The problem considered here is to obtain the optimal coherent sensor structures for the channels. A theorem is proven in section 4.3.1, and a non-linear integer programming (NLIP) problem is devised to minimize an expected total loss. The extended Lawler and Bell's method is applied to the resulting problem through a coordinate transformation. An illustrative example of a three-channel safety monitoring system is given to show this procedure in detail.

4.2 PROBLEM STATEMENT

4.2.1 Assumptions

1 The safety monitoring system is composed of N channels.

2 Channel i is a coherent structure of n_i identical sensors of type i.

3 Each channel supervises a specific plant state.

4 The logic structure between channels is specified.

5 Sensors fail s-independently.

4.2.2 Notation

X_i binary indicator variable for plant state i.

$$X_i = \begin{cases} 1, & \text{if plant state i is abnormal,} \\ 0, & \text{otherwise.} \end{cases}$$

$\underline{X}$ $(X_1,\ldots,X_N)$

Y_{ij} binary indicator variable for sensor j of type i.

$$Y_{ij} = \begin{cases} 1, & \text{if sensor j of type i is yielding the sensor alarm,} \\ 0, & \text{otherwise.} \end{cases}$$

$\underline{Y}_i$ $(Y_{i1},\ldots,Y_{iN_1})$

Z_i binary indicator variable for channel i.

$$Z_i = \begin{cases} 1, & \text{if channel i is yielding the channel alarm,} \\ 0, & \text{otherwise.} \end{cases}$$

$\underline{Z}$ $(Z_1,\ldots,Z_N)$

q_{1i} conditional FD probability of a sensor of type i.

q_{2i} conditional FS probability of a sensor of type i.

Q_{1i} $\Pr\{Z_i=0|X_i=1\}$: conditional FD probability of channel i

Q_{2i} $\Pr\{Z_i=1|X_i=0\}$: conditional FS probability of channel i

$\underline{1-q}_{1i}$ $(1-q_{1i},\ldots,1-q_{1i})$

$\underline{q}_{2i}$ $(q_{2i},\ldots,q_{2i})$

$h_i(\underline{Y}_i)$ reliability function of channel i

$C(\underline{X},\underline{Z})$ loss function of plant states and channel output states, indicating loss caused by failures of the safety monitoring system.

n_i, k_i decision variables specifying k_i-out-of-n_i:G structure

$\underline{n}$ $(n_1,\ldots,n_N)$

$\underline{k}$ $(k_1,\ldots,k_N)$

n_{io} upper bound of n_i

c_{si} cost of sensor i

C_{SO} upper bound of total investment cost for sensors

I_S s-expected total loss caused by the failures of the safety monitoring system

binfc(k;p,N) survivor function of binomial distribution;

$$\text{binfc}(k;p,N) = \sum_{i=k}^{N} \binom{N}{i} p^i (1-p)^{N-i}.$$

From assumption 2, the FD and FS probabilities; Q_{1i} and Q_{2i} are:

$$Q_{1i} = 1 - h_i(\underline{1}-\underline{q}_{1i}), \tag{1}$$

$$Q_{2i} = h_i(\underline{q}_{2i}). \tag{2}$$

The problem is to obtain, for each channel, the coherent structure that minimizes an s-expected total loss caused by failures of the safety monitoring system.

4.3 PROBLEM SOLUTION

4.3.1 NLIP Problem Formulation

The s-expected total loss is the sum of losses over all the plant states and channel states:

$$I_S = \sum_{\underline{X}} \sum_{\underline{Z}} C(\underline{X},\underline{Z}) \Pr\{\underline{Z}\} \Pr\{\underline{Z}|\underline{X}\}. \tag{3}$$

The constant $C(\underline{X},\underline{Z})$ can be specified when the plant state $\underline{X}$ and the channel state $\underline{Z}$ are known. See Table 4.2 for example.

From assumption 4,

$$\Pr\{\underline{Z}|\underline{X}\} = \prod_{i=1}^{N} \Pr\{Z_i|X_i\}.$$

Since $\Pr\{Z_i|X_i\} = X_i[\, Z_i\Pr\{Z_i=1|X_i=1\} + (1-Z_i)\Pr\{Z_i=0|X_i=1\}\,] + (1-X_i)[\, Z_i\Pr\{Z_i=1|X_i=0\} + (1-Z_i)\Pr\{Z_i=0|X_i=0\}\,]$, $Q_{1i} = \Pr\{Z_i=0|X_i=1\}$, and $Q_{2i} = \Pr\{Z_i=1|X_i=0\}$, we have

$$\Pr\{\underline{Z}|\underline{X}\} = \prod_{i=1}^{N} [X_i\{Z_i(1-Q_{1i})+(1-Z_i)Q_{1i}\} + (1-X_i)\{Z_iQ_{2i}+(1-Z_i)(1-Q_{2i})\}]. \quad (4)$$

From eqs. (3) and (4), the s-expected total loss I_S is a multi-linear function of the FD and FS failure probabilities of the channels. It further satisfies

$$\frac{\partial^2 I_S}{\partial Q_{1i}\partial Q_{2i}} = 0, \quad \text{for all } i. \quad (5)$$

The following theorem holds for a multi-linear function which meets the requirement of eq. (5).

THEOREM :

Let $F(\underline{Q}_1,\underline{Q}_2)$ be a multi-linear function satisfying $\partial^2 F/\partial Q_{1i}\partial Q_{2i} = 0$, for all i. In the opitmal safety monitoring system that minimizes $F(\underline{Q}_1,\underline{Q}_2)$, each channel forms k-out-of-n:G structure.

Proof :

From the assumption in the theorem,

$$F = F_{1i}Q_{1i} + F_{2i}Q_{2i} + F_{3i}, \qquad (6)$$

where F_{1i}, F_{2i}, and F_{3i} are multi-linear functions of FD and FS probabilities except Q_{1i} and Q_{2i}. If the structure of the channels except channel i are fixed, then F_{1i}, F_{2i}, and F_{3i} are constant. According to the appendix in [P2], a reliability function $h(\underline{Y})$ of any coherent structure composed of n identical components can be expressed as

$$h(\underline{Y}) = \sum_{k=1}^{n} a_k u_{k,n}(\underline{Y}), \text{ for } a_k \geq 0,\ k=1,\ldots,n \text{ and } \sum_{k=1}^{n} a_k = 1, \qquad (7)$$

where $u_{k,n}(\underline{Y})$: reliability function of k-out-of-n:G structure.

From eqs. (1), (2), (6) and (7),

$$F = F_{1i}\{ 1 - \sum_{k=1}^{n_i} a_k u_{k,n_i}(\underline{1}-\underline{q}_{1i}) \} + F_{2i}\{ \sum_{k=1}^{n_i} a_k u_{k,n_i}(\underline{q}_{2i}) \} + F_{3i}$$

$$= \sum_{k=1}^{n_i} a_k \{ F_{1i} - F_{1i}u_{k,n_i}(\underline{1}-\underline{q}_{1i}) + F_{2i}u_{k,n_i}(\underline{q}_{2i}) + F_{3i} \}$$

$$\geq \min_k \{ F_{1i} - F_{1i}u_{k,n_i}(\underline{1}-\underline{q}_{1i}) + F_{2i}u_{k,n_i}(\underline{q}_{2i}) + F_{3i} \}, \qquad (8)$$

where $\min_k \{ a_k \}$ indicates the minimum of a_k with respect to k.

Thus, the optimal structure of channel i must be k_i-out-of-n_i:G structure. The theorem can be proven by induction on the channels.

Q.E.D.

According to the theorem, channel i can be assumed to be k_i-out-of-n_i:G structure, and the problem can be formulated as:

PROBLEM :

$$\text{Minimize :} \quad \underset{\underline{n},\underline{k}}{} \quad I_S$$

$$\text{subject to:} \quad \sum_{i=1}^{N} c_{si} n_i \leq C_{SO},$$

$$n_i \leq n_{io}, \quad i = 1,\ldots,N.$$

$$Q_{1i} = 1 - \text{binfc}(k_i; 1-q_{1i}, n_i), \quad i = 1,\ldots,N, \qquad (9)$$

$$Q_{2i} = \text{binfc}(k_i; q_{2i}, n_i), \quad i = 1,\ldots,N. \qquad (10)$$

4.3.2 Solution Method

Eqs. (9) and (10) indicate that Q_{1i} is monotone increasing with respect to k_i, and that Q_{2i} is monotone decreasing in k_i. Simple calculations in Appendix 1 shows that Q_{1i} is monotone decreasing in n_i, and that Q_{2i} is monotone decreasing in n_i. Converting k_i to $n_{io}+1-k_i'$, Q_{1i} becomes monotone decreasing in k_i' and Q_{2i} becomes monotone increasing in k_i'. Thus, Q_{1i} is monotone decreasing and Q_{2i} is monotone increasing with respect to n_i and k_i', i=1,...,N.

Since I_S is a multi-linear function of Q_{1i} and Q_{2i}, I_S can be expressed by a sum of products of Q_{1i} and Q_{2i}, i=1,...,N. Applying the transformation rules in Table 4.1 to the sum of products expression, I_S can be written in the form:

$f_1(\underline{n},\underline{k}') - f_2(\underline{n},\underline{k}')$ where f_1 and f_2 are monotone increasing in each variable.

The constraint functions can be also transformed into the above form. Thus, the problem can be solved by the extended Lawler and Bell's method [M1].

4.4 ILLUSTRATIVE EXAMPLE

Table 4.1 Transformation rule: $f(\underline{X}) = f_1(\underline{X}) - f_2(\underline{X})$

$f(\underline{X})$	$f_1(\underline{X})$	$f_2(\underline{X})$
$g(\underline{X})h(\underline{X})$	$cg(\underline{X})$	$g(\underline{X})\{c-h(\underline{X})\}$
$-g(\underline{X})h(\underline{X})$	$g(\underline{X})\{c-h(\underline{X})\}$	$cg(\underline{X})$

Notes:

1. $f_1(\underline{X})$, $f_2(\underline{X})$: monotone increasing
2. $g(\underline{X})$: monotone increasing (≥ 0)
3. $h(\underline{X})$: monotone decreasing
4. c: positive constant ($\geq \max_{\underline{X}} h(\underline{X})$)

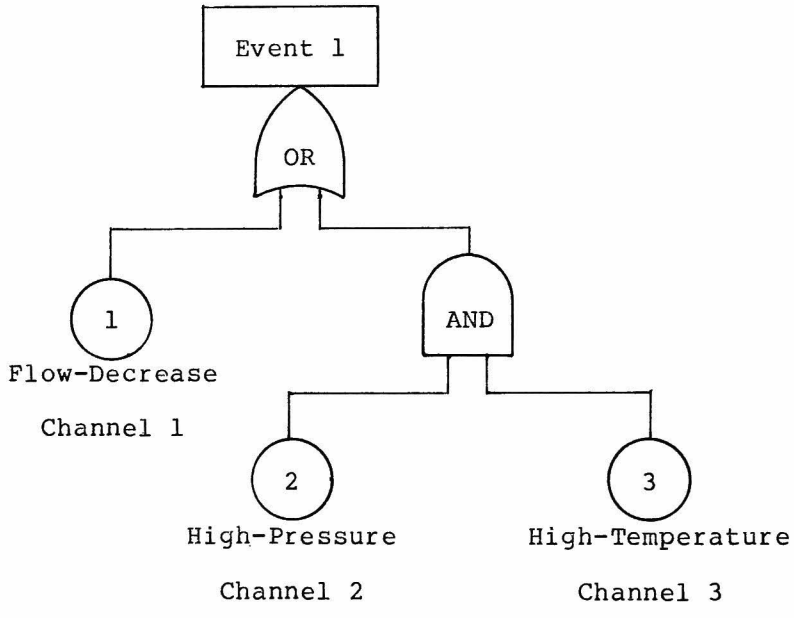

Fig. 4.1 Single-event safety monitoring system

Table 4.2 Losses caused by the failures of the safety monitoring system

(Y_1,Y_2,Y_3)	(0,0,0)	(0,0,1)	(0,1,0)	(0,1,1)	(1,0,0)	(1,0,1)	(1,1,0)	(1,1,1)
(X_1,X_2,X_3)								
(0,0,0)	0	0	0	C_{2S}	C_{2S}	C_{2S}	C_{2S}	C_{2S}
(0.0.1)	0	0	0	C_{2S}	C_{2S}	C_{2S}	C_{2S}	C_{2S}
(0.1.0)	0	0	0	C_{2S}	C_{2S}	C_{2S}	C_{2S}	C_{2S}
(0,1,1)	C_{1S}	C_{1S}	C_{1S}	0	0	0	0	0
(1,0,0)	C_{1S}	C_{1S}	C_{1S}	0	0	0	0	0
(1,0,1)	C_{1S}	C_{1S}	C_{1S}	0	0	0	0	0
(1,1,0)	C_{1S}	C_{1S}	C_{1S}	0	0	0	0	0
(1,1,1)	C_{1S}	C_{1S}	C_{1S}	0	0	0	0	0

Table 4.3 Probabilities of channel states for a given plant state

X_1	X_2	X_3	Y_1	Y_2	Y_3	$Pr\{\underline{Y}\|\underline{X}\}$
0	0	0	0	1	1	$(1-Q_{21})Q_{22}Q_{23}$
			1	0	0	$Q_{21}(1-Q_{22})(1-Q_{23})$
			1	0	1	$Q_{21}(1-Q_{22})Q_{23}$
			1	1	0	$Q_{21}Q_{22}(1-Q_{23})$
			1	1	1	$Q_{21}Q_{22}Q_{23}$
0	0	1	0	1	1	$(1-Q_{21})Q_{22}(1-Q_{13})$
			1	0	0	$Q_{21}(1-Q_{22})Q_{13}$
			1	0	1	$Q_{21}(1-Q_{22})(1-Q_{13})$
			1	1	0	$Q_{21}Q_{22}Q_{13}$
			1	1	1	$Q_{21}Q_{22}(1-Q_{13})$
0	1	0	0	1	1	$(1-Q_{21})(1-Q_{12})Q_{23}$
			1	0	0	$Q_{21}Q_{12}(1-Q_{23})$
			1	0	1	$Q_{21}Q_{12}Q_{23}$
			1	1	0	$Q_{21}(1-Q_{12})(1-Q_{23})$
			1	1	1	$Q_{21}(1-Q_{12})Q_{23}$
0	1	1	0	0	0	$(1-Q_{21})Q_{12}Q_{13}$
			0	0	1	$(1-Q_{21})Q_{12}(1-Q_{13})$
			0	1	0	$(1-Q_{21})(1-Q_{12})Q_{13}$
1	0	0	0	0	0	$Q_{11}(1-Q_{22})(1-Q_{23})$

			0	0	1	$Q_{11}(1-Q_{22})Q_{23}$
			0	1	0	$Q_{11}Q_{22}(1-Q_{23})$
1	0	1	0	0	0	$Q_{11}(1-Q_{22})Q_{13}$
			0	0	1	$Q_{11}(1-Q_{22})(1-Q_{13})$
			0	1	0	$Q_{11}Q_{22}Q_{13}$
1	1	0	0	0	0	$Q_{11}Q_{12}(1-Q_{23})$
			0	0	1	$Q_{11}Q_{12}Q_{23}$
			0	1	0	$Q_{11}(1-Q_{12})(1-Q_{23})$
1	1	1	0	0	0	$Q_{11}Q_{12}Q_{13}$
			0	0	1	$Q_{11}Q_{12}(1-Q_{13})$
			0	1	0	$Q_{11}(1-Q_{12})Q_{13}$

Consider a single-event safety monitoring system shown in Fig. 4.1. An inadvertent event is defined as {Flow-Decrease} OR {High-Pressure AND High-Temperature}. Channels 1, 2, and 3 monitor flow-decrease, high-pressure, and high-temperature, respectively. If {channel 1} OR {channel 2 AND channel 3} detect abnormal plant states, then the safety monitoring system yields a system alarm and activates an appropriate safety system. Table 4.2 shows losses over all the plant states and the channel states. The FD loss: C_{1S} is caused if the inadvertent event takes place with the safety monitoring system yielding no system alarms. On the other hand, the FS loss: C_{2S} is caused when the safety monitoring system generates a spurious system alarm, the plant being normal. Table 4.3 shows the probabilities of the plant states and the channel states, under which either FD or FS loss is caused. As discussed in section 4.3.2, the s-expected total loss I_S is a multi-linear function of Q_{1i} and Q_{2i}, satisfying $\partial^2 I_S/\partial Q_{1i}\partial Q_{2i} = 0$. Expanding I_S as the sum of products of Q_{1i} and Q_{2i}, every term can be written in one of the following three forms:

a) a product of only Q_{1i},

b) a product of only Q_{2j}, and

c) a product of Q_{1i} and Q_{2j}.

A term in the form of a) or b) has the monotone property with respect to n_i and k_i'. Since $Q_{1i} = 1 - (1-Q_{1i})$ and $Q_{2j} = 1 - (1-Q_{2j})$, a product term in the form of c) can be transformed into a sum of products which are:

1) a product of Q_{1i},

2) a product of Q_{2j},

3) a product of Q_{1i} and $(1-Q_{2j})$, and

4) a product of Q_{2j} and $(1-Q_{1i})$.

All these terms also have the monotone property. Thus, the s-expected total loss I_S can be written as:

$I_S = f_{o1} - f_{o2}$,

where

$$\begin{aligned} f_{o1} = \; & C_{2S}[\, Pr\{\underline{X}=(0,0,0)\}(Q_{21}+Q_{22}Q_{23}) \\ & + Pr\{\underline{X}=(0,0,1)\}\{Q_{22}(1-Q_{13})+Q_{21}\} \\ & + Pr\{\underline{X}=(0,1,0)\}\{(1-Q_{12})Q_{23}+Q_{21}\}\,] \\ & - C_{1S}[\, Pr\{\underline{X}=(0,1,1)(1-Q_{21})Q_{12}Q_{13} \\ & + Pr\{\underline{X}=(1,0,0)\}Q_{11}(1-Q_{22})(1-Q_{23}) \\ & + Pr\{\underline{X}=(1,0,1)\}Q_{11}(1-Q_{22})Q_{13} \\ & + Pr\{\underline{X}=(1,1,0)\}Q_{11}Q_{12}(1-Q_{23}) \\ & + Pr\{\underline{X}=(1,1,1)\}Q_{11}Q_{12}Q_{13}\,] \end{aligned} \tag{12}$$

$$\begin{aligned} f_{o2} = \; & C_{2S}[\, Pr\{\underline{X}=(0,0,0)\}Q_{21}Q_{22}Q_{23} \\ & + Pr\{\underline{X}=(0,0,1)\}Q_{21}Q_{22}(1-Q_{13}) \\ & + Pr\{\underline{X}=(0,1,0)\}Q_{21}(1-Q_{12})Q_{23}\,] \\ & - C_{1S}[\, Pr\{\underline{X}=(0,1,1)\}\{(1-Q_{21})Q_{12}+(1-Q_{21})Q_{13}\} \\ & + Pr\{\underline{X}=(1,0,0)\}\{Q_{11}(1-Q_{22})+Q_{11}(1-Q_{23})\} \\ & + Pr\{\underline{X}=(1,0,1)\}\{Q_{11}(1-Q_{22})+Q_{11}Q_{13}\} \\ & + Pr\{\underline{X}=(1,1,0)\}\{Q_{11}Q_{12}+Q_{11}(1-Q_{23})\} \\ & + Pr\{\underline{X}=(1,1,1)\}\{Q_{11}Q_{12}+Q_{11}Q_{13}\}. \end{aligned} \tag{13}$$

The functions f_{o1} and f_{o2} are monotone increasing in each of decision variables; n_i, k_i', i=1,2,3. The data in Tables 4.4 and

Table 4.4 Probabilities of plant states

X_1	X_2	X_3	$Pr\{\underline{X}\}$
0	0	0	0.980
0	0	1	0.002
0	1	0	0.002
0	1	1	0.004
1	0	0	0.002
1	0	1	0.003
1	1	0	0.003
1	1	1	0.004

Table 4.5 Values of q_{1i}, q_{2i}, c_{si}, n_{io}, C_{SO}, C_{1S}, & C_{2S}

i	1	2	3	
q_{1i}	0.003	0.001	0.005	C_{1S} = 10000
q_{2i}	0.006	0.005	0.010	C_{2S} = 100
c_{si}	6	8	4	C_{SO} = 40
n_{io}	4	4	4	

4.5 are assumed. The optimal structure for each channel is:

Channel 1: 2-out-of-3:G structure,

Channel 2: 1-out-of-1:G structure,

Channel 3: 2-out-of-3:G structure,

and the minimum of I_S is 17.976. The total investment cost is 38.

APPENDIX

1 Property of Q_{1i} and Q_{2i} with respect to n_i

From eqs. (9) and (10),

$$Q_{1i} = \sum_{j=0}^{k_i-1} \binom{n_i}{j} (1-q_{1i})^j q_{1i}^{n_i-j},$$

$$Q_{2i} = 1 - \sum_{j=0}^{k_i-1} \binom{n_i}{j} q_{2i}^j (1-q_{2i})^{n_i-j}.$$

Let dQ_{1i} be the perturbation in Q_{1i} when n_i changes to n_i+1. Then,

$$dQ_{1i} = \sum_{j=0}^{k_i-1} \binom{n_i+1}{j} (1-q_{1i})^j q_{1i}^{n_i+1-j} - \sum_{j=0}^{k_i-j} \binom{n_i}{j} (1-q_{1i})^j q_{1i}^{n_i-j}.$$

Since $\binom{n+1}{i} = \binom{n}{i} + \binom{n}{i-1}$ and $\binom{n+1}{0} = \binom{n}{0}$, we have

$$dQ_{1i} = \sum_{j=1}^{k_i-1} \left[\left\{ \binom{n_i}{j} + \binom{n_i}{j-1} \right\} (1-q_{1i})^j q_{1i}^{n_i+1-j} - \binom{n_i}{j} (1-q_{1i})^j q_{1i}^{n_i-j} \right]$$

$$+ \binom{n_i}{0} q_{1i}^{n_i+1} - \binom{n_i}{0} q_{1i}^{n_i}$$

$$= \sum_{j=0}^{k_i-2} \binom{n_i}{j} (1-q_{1i})^{j+1} q_{1i}^{n_i-j} - \sum_{j=0}^{k_i-1} \binom{n_i}{j} (1-q_{1i})^{j+1} q_{1i}^{n_i-j}$$

$$= - \binom{n_i}{k_i-1} (1-q_{1i})^{k_i} q_{1i}^{n_i+1-k_i} < 0.$$

Similarly, let dQ_{2i} be the perturbation in Q_{2i} when n_i changes to n_i+1. Then,

$$dQ_{2i} = \{ 1 - \sum_{j=0}^{k_i-1} \binom{n_i+1}{j} q_{2i}^{\,j} (1-q_{2i})^{n_i+1-j} \}$$

$$- \{ 1 - \sum_{j=0}^{k_i-1} \binom{n}{j} i) q_{2i}^{\,j} (1-q_{2i})^{n_i-j} \}$$

$$= \binom{n_i}{k_i-1} q_{2i}^{\,k_i} (1-q_{2i})^{n_i+1-k_i} > 0.$$

Thus, Q_{1i} is monotone decreasing in n_i and Q_{2i} is monotone increasing in n_i.

2 Extended Lawler and Bell's Method [M1]

The extended Lawler and Bell's method can be applied to an NLIP problem, that can be put into the form:

Minimize: $f_{o1}(\underline{X}) - f_{o2}(\underline{X})$,

subject to: $f_{j1}(\underline{X}) - f_{j2}(\underline{X}) \geq 0, \quad j = 1,\ldots,m,$

where 1) $\underline{X} = (X_1,\ldots,X_n)$ and $S_i \leq X_i \leq M_i$ for S_i, M_i, X_i $Z^+ = \{0,1,2,\ldots.\}$, $i=1,\ldots,n$.

2) f_{o1}, f_{o2}, f_{j1}, and f_{j2} $(j=1,\ldots,m)$ are monotone increasing in each of the decision variable.

Let us use the same notations as in [S1]. The method obtains the optimal solution by examining part of $\Pi_{i=1}^{n}(M_i-S_i+1)$ possible solutions in a numerical order [L1], beginning with $\underline{X} = (S_1,\ldots,S_n)$ and ending with $\underline{X} = (M_1,\ldots,M_n)$. Let $\underline{X}$ denote the vector that is currently being examined, and let $\underline{X}^o$ be the optimal solution among the vector that have been examined. The method is described as follows:

Step 1: If $f_{o1}(\underline{X}^+) - f_{o2}(\underline{X}) \geq f_{o1}(\underline{X}^o) - f_{o2}(\underline{X}^o)$, then skip to $\underline{X}^*$. Otherwise, go to step 2.

Step 2: If $f_{j1}(\underline{X}^+) - f_{j2}(\underline{X}) < 0$, for some j, then skip to $\underline{X}^*$. Otherwise, go to step 3.

Step 3: If $f_{o1}(\underline{X}) - f_{o2}(\underline{X}) \geq f_{o1}(\underline{X}^{o}) - f_{o2}(\underline{X}^{o})$, then skip to $\underline{X}^{++}$. Otherwise, go to step 4.

Step 4: If $f_{j1}(\underline{X}) - f_{j2}(\underline{X}) < 0$, for some j, then skip to $\underline{X}^{++}$. Otherwise, let $\underline{X}^{o}$ be $\underline{X}$ and skip to $\underline{X}^{++}$.

The method terminates the search when $\underline{X}^{++}$ or $\underline{X}^{*}$ is greater than $\underline{X}_{max} = (M_1,\ldots,M_n)$ in the numerical order.

CHAPTER 5

OPTIMAL BOOLEAN STRUCTURE

OF

ONE-PLANT-STATE MONITORING SYSTEMS

5.1 INTRODUCTION

Considering common-mode failures among sensors, it is better to use several kinds of sensors for monitoring the state of the plant. However, through CHAPTERS 3 and 4 we assumed coherent structures and channels of identical sensors. From this chapter on, we extend the optimal structure design to cases involving not only general components, but also non-coherent structures.

A Boolean structure is equivalent to a truth table. Thus, the number of structures composed of n components is equal to $_2 2^n$. Table 5.1 shows the cases where n ranges from 1 to 5. The structures remarkably increase as the more components become available. A simple termwise search for the optimal structure is thus impractical. A new method should be developed.

This chapter considers the safety monitoring system where all the sensors supervise a specific state of the plant. A simple rule to determine the optimal structure is devised in section 5.3.1. Three properties of the optimal structure are then derived

Table 5.1 Number of Boolean structures

n	number of structures
1	4
2	16
3	256
4	65536
5	4294967304

in section 5.3.2, considering sensor reliabilities; a non-coherent structure can be optimal in some case. In section 5.3.3, a systematic method is applied to determine the optimal structure. This requires at most 2^n simple iterations, rather than ${}_2 2^n$. Analytic solutions are obtained in section 5.3.4 where simplification of the expression of the optimal structure is also discussed. An illustrative example in section 5.4 shows that using more sensors is not necessarily better in terms of minimizing an s-expected total loss.

5.2 PROBLEM STATEMENT

5.2.1 Assumptions

1 The safety monitoring system is composed of n sensors, which are not necessarily identical.

2 All the sensors supervise a specific state of the plant.

3 Sensors fail s-independently.

5.2.2 Notation

Y_i binary indicator variable for sensor i

$$Y_i = \begin{cases} 1, & \text{if sensor i is generating the sensor alarm,} \\ 0, & \text{otherwise.} \end{cases}$$

$\underline{Y}$ $(Y_1,\ldots,Y_n)$

$\underline{Y}(i)$ $(Y_1,\ldots,Y_{i-1},Y_{i+1},\ldots,Y_n)$

$a_i:\underline{Y}(i)$ $(Y_1,\ldots,Y_{i-1},a,Y_{i+1},\ldots,Y_n)$

$f(\underline{Y})$ structure function of the safety monitoring system

$$f(\underline{Y}) = \begin{cases} 1, & \text{if the safety monitoring system is generating the system alarm,} \\ 0, & \text{otherwise.} \end{cases}$$

$h(\underline{Y})$ reliability function of the safety monitoring system

q_{1i} conditional FD probability of sensor i

$\underline{1-q_1}$ $(1-q_{11},\ldots,1-q_{1n})$

q_{2i} conditional FS probability of sensor i

$\underline{q_2}$ $(q_{21},\ldots,q_{2n})$

Q_{1S} conditional FD probability of the safety monitoring system

Q_{2S} conditional FS probability of the safety monitoring system

P probability that the plant state is abnormal

C_{1S} FD loss: loss caused when the safety monitoring system fails to generate the system alarm, given inadvertent plant state in the plant

C_{2S} FS loss: loss caused when the safety monitoring system generates a spurious system alarm, given that the inadvertent plant state does not exist in the plant

c_{si} cost of sensor i

C_{SO} upper bound of total investment cost available for sensors

I_S s-expected total loss caused by failures of the safety monitoring system

INT[k] minimum integer that is larger than or equal to k; for a positive integer k, INT[k] can be either k or k+1.

From assumptions 2 and 3, the probabilities Q_{1S} and Q_{2S} are:

$$Q_{1S} = 1 - h(\underline{1-q_1}), \tag{1}$$

$$Q_{2S} = h(\underline{q_2}). \tag{2}$$

The s-expected total loss I_S is the same as that in CHAPTER 3:

$$I_S = C_{1S}PQ_{1S} + C_{2S}(1-P)Q_{2S}. \tag{3}$$

The problem is to determine the structure function $f(\underline{Y})$ that

minimizes I_S among all the Boolean structures.

5.3 PROBLEM SOLUTION

5.3.1 Optimal Boolean Structure of One-Plant-State Monitoring Systems

The reliability function of any Boolean structure composed of n sensors is expressed as eq. (2) of CHAPTER 2:

$$h(\underline{Y}) = \sum_{\underline{X}} f(\underline{X}) \left[\prod_{i=1}^{n} \{ X_i Y_i + (1-X_i)(1-Y_i) \} \right], \tag{4}$$

where the sum is extended over all the binary vector $\underline{X}=(X_1,\ldots,X_n)$.

From eqs. (1)-(4),

$$I_S = C_{1S}P - \sum_{\underline{Y}} f(\underline{Y}) \left[C_{1S}P \prod_{i=1}^{n} \{Y_i(1-q_{1i})+(1-Y_i)q_{1i}\} \right.$$

$$\left. - C_{2S}(1-P) \prod_{i=1}^{n} \{Y_i q_{2i}+(1-Y_i)(1-q_{2i})\} \right]. \tag{5}$$

Define $g(\underline{Y})$ as

$$g(\underline{Y}) = C_{1S}P \prod_{i=1}^{n} \{Y_i(1-q_{1i})+(1-Y_i)q_{1i}\}$$

$$- C_{2S}(1-P) \prod_{i=1}^{n} \{Y_i q_{2i}+(1-Y_i)(1-q_{2i})\}. \tag{6}$$

Then,

$$I_S = C_{1S}P - \sum_{\underline{Y}} f(\underline{Y}) g(\underline{Y}). \tag{7}$$

The first term on the right hand side of eq. (7) indicates the loss caused in the plant without the safety monitoring system. The second term implies the reduction of the loss through the application of the safety monitoring system. If we set $f(\underline{Y}) = 1$

for any $\underline{Y}$ satisfying $g(\underline{Y}) > 0$, then I_S attains its minimum. The optimal structure $f^*(\underline{Y})$ is:

$$f^*(\underline{Y}) = \begin{cases} 1, & \text{if } g(\underline{Y}) > 0, \\ 0, & \text{otherwise.} \end{cases} \tag{8}$$

We call $g(\underline{Y})$ the switching function of the optimal structure $f^*(\underline{Y})$. This structure is optimal among all the Boolean structures. The optimal $f^*(\underline{Y})$ can be expressed as:

$$f^*(\underline{Y}) = \sum_{\underline{Z} \in P} \{ \prod_{i=1}^{n} Y_i(Z_i) \}, \tag{9}$$

where

$$P = \{ \underline{Y} \mid g(\underline{Y}) > 0 \}, \tag{10}$$

$$Y_i(Z_i) = \begin{cases} Y_i, & \text{if } Z_i = 1, \\ \overline{Y}_i, & \text{otherwise.} \end{cases} \tag{11}$$

Here set P implies the set of path vectors of $f^*(\underline{Y})$.

5.3.2 Simplification of Optimal Boolean Structure Function

The function $g(\underline{Y})$ has the following property.

PROPERTY :

(P1) If $q_{1i} + q_{2i} \leq 1$ and $g(0_i:\underline{Y}(i)) > 0$, then $g(1_i:\underline{Y}(i)) > 0$.

(P2) If $q_{1i} + q_{2i} > 1$ and $g(1_i:\underline{Y}(i)) > 0$, then $g(0_i:\underline{Y}(i)) > 0$.

Proof :

From eq. (6), $g(0_i:\underline{Y}(i))$ and $g(1_i:\underline{Y}(i))$ can be written as:

$$g(0_i:\underline{Y}(i)) = C_1 q_{1i} - C_2(1-q_{2i}), \tag{12}$$

$$g(1_i:\underline{Y}(i)) = C_1(1-q_{1i}) - C_2 q_{2i}, \tag{13}$$

where

$$C_1 = C_{1S}^{P} \prod_{j \neq i} \{Y_j(1-q_{1j}) + (1-Y_j)q_{1j}\},$$

$$C_2 = C_{2S}^{(1-P)} \prod_{j \neq i} \{Y_j q_{2j} + (1-Y_j)(1-q_{2j})\}.$$

We now prove the property (P1) first. Since $g(0_i:\underline{Y}(i)) > 0$, the following inequality holds:

$$\frac{C_2(1-q_{2i})}{C_1 q_{1i}} < 1. \tag{14}$$

Factoring $C_1(1-q_{1i})$ out of the right hand side of eq. (13), we have

$$g(1_i:\underline{Y}(i)) = C_1(1-q_{1i})\{\, 1 - \frac{C_2 q_{2i}}{C_1(1-q_{1i})} \,\}.$$

Eq. (14) and the assumption: $q_{1i} + q_{2i} \leq 1$, yield the inequality:

$$\frac{C_2 q_{2i}}{C_1(1-q_{1i})} = \frac{C_2(1-q_{2i})}{C_1 q_{1i}} \times \frac{q_{1i}}{1-q_{2i}} \times \frac{q_{2i}}{1-q_{1i}} < 1.$$

Thus, $g(1_i:\underline{Y}(i)) > 0$ is proven. The property (P2) can be proven in a similar way.

Q.E.D.

This property shows that the function $g(\underline{Y})$ has a different property depending on whether $q_{1i} + q_{2i} \leq 1$ or not. So we consider the optimal structure in the following three cases, respectively:

Case 1: $q_{1i} + q_{2i} \leq 1$, for $i=1,\ldots,n$.

Case 2: $q_{1i} + q_{2i} > 1$, for $i=1,\ldots,n$.

Case 3: $q_{1i} + q_{2i} \leq 1$, for $i=1,\ldots,n_1$, and $q_{1i} + q_{2i} > 1$, for $i=n_1+1,\ldots,n$.

1) Case 1

The property (P1) shows that $g(\underline{Y}) > 0$ implies $g(\underline{Y}') > 0$ for any $\underline{Y}' \geq \underline{Y}$. We see from eq. (8) that the optimal structure

function $f^*(\underline{Y})$ is monotone increasing:

$\underline{Y} \leq \underline{Y}' \quad ====> \quad f(\underline{Y}) \leq f(\underline{Y}')$.

Define subset P_1^* of set P by

$$P_1^* = \{ \underline{Y} \mid g(\underline{Y}) > 0 \text{ and if } \underline{Y} > \underline{Y}', \text{ then } g(\underline{Y}') \leq 0 \}, \tag{15}$$

The set P_1^* is the set of minimal path vectors of the optimal structure. Each minimal path set of the optimal structure $f^*(\underline{Y})$ now becomes a subset of $\{1,2,\ldots,n\}$, because the optimal structure satisfy the most essential requirement of the coherent structure, i.e., "monotone property" (see section 2.4 of CHAPTER 2). Thus,

$$f^*(\underline{Y}) = \coprod_{\underline{Z} \in P_1^*} \{ \prod_{j \in C_1(\underline{Z})} Y_j \}. \tag{16}$$

where

$$C_1(\underline{Z}) = \{ i \mid Z_i = 1 \}. \tag{17}$$

2) Case 2

The property (P2) shows that $g(\underline{Y}) > 0$ implies $g(\underline{Y}') > 0$ for any $\underline{Y}' \leq \underline{Y}$. On the contrary to Case 1, the optimal structure function $f^*(\underline{Y})$ is monotone decreasing:

$\underline{Y} \leq \underline{Y}' \quad ====> \quad f^*(\underline{Y}) \geq f^*(\underline{Y}')$.

Define subset P_2^* of set P by

$$P_2^* = \{ \underline{Y} \mid g(\underline{Y}) > 0 \text{ and if } \underline{Y} < \underline{Y}', \text{ then } g(\underline{Y}') \leq 0 \}. \tag{18}$$

The set P_2^* corresponds to the set P_1^* in Case 1. In this case, each minimal path set of the optimal structure $f^*(\underline{Y})$ becomes a subset of $\{\bar{1},\bar{2},\ldots,\bar{n}\}$, because the optimal structure has monotone decreasing property. Thus, the optimal structure $f^*(\underline{Y})$ is:

$$f^*(\underline{Y}) = \coprod_{\underline{Z} \in P_2^*} \{ \prod_{j \in C(\underline{Z})} \bar{Y}_j \}, \tag{19}$$

where

$$C_0(\underline{Z}) = \{ i \mid Z_i = 0 \}. \tag{20}$$

Note that the optimal structure becomes non-coherent.

3) Case 3

This is a combination of Case 1 and Case 2. Let $\underline{Y}_1$ denote $(Y_1,\ldots,Y_{n_1})$ and $\underline{Y}_2$ denote $(Y_{n_1+1},\ldots,Y_n)$. Then, the property proves the following two implications.

1. $g(\underline{Y}_1,\underline{Y}_2) > 0 \quad ====> \quad g(\underline{Y}_1',\underline{Y}_2) > 0.$ if $\underline{Y}_1' \geq \underline{Y}_1$,

2. $g(\underline{Y}_1,\underline{Y}_2) > 0 \quad ====> \quad g(\underline{Y}_1,\underline{Y}_2') > 0,$ if $\underline{Y}_1' \leq \underline{Y}_2$.

Hence, the optimal structure function $f^*(\underline{Y}_1,\underline{Y}_2)$ is monotone increasing with respect to $\underline{Y}_1$, while it is monotone decreasing with respect to $\underline{Y}_2$. The following set P_3^* can be defined as

$$P_3^* = \{ (\underline{Y}_1,\underline{Y}_2) \mid g(\underline{Y}_1,\underline{Y}_2)>0 \text{ and; if } \underline{Y}_1 > \underline{Y}_1', \text{ then } g(\underline{Y}_1',\underline{Y}_2) \leq 0 \text{ and; if } \underline{Y}_2' > \underline{Y}_2, \text{ then } g(\underline{Y}_1,\underline{Y}_2') \leq 0 \} \quad (21)$$

Each minimal path set in this case is a subset of $\{1,\ldots,n_1,\overline{n_1+1},\ldots,\overline{n}\}$. The optimal structure function $f^*(\underline{Y}_1,\underline{Y}_2)$ can be expressed by

$$f^*(\underline{Y}_1,\underline{Y}_2) = \coprod_{(\underline{Z}_1,\underline{Z}_2)\in P_3^*} \{ (\prod_{j\in C_1(\underline{Z}_1)} Y_j)(\prod_{k\in C_0(\underline{Z}_2)} \overline{Y}_k) \}. \quad (22)$$

5.3.3 Systematic Method of Obtaining Minimal Path Sets

When a functional form of $f^*(\underline{Y})$ is given, we can implement the logic $f^*(\underline{Y})$ as a hard-wired circuit or as a computer program. In order to obtain the functional form of $f^*(\underline{Y})$, we must obtain the minimal path sets. Then, we propose a systematic method to obtain the minimal path sets.

Consider Case 3 in section 5.3.2 as a general case. Obtaining the minimal path sets is equivalent to obtaining the set P_3^*. Converting $\underline{Y}_2$ to $\underline{1-Y}_2'$, $g(\underline{Y}_1,\underline{Y}_2')$ becomes now monotone increasing with respect to $(\underline{Y}_1,\underline{Y}_2')$. Hence, we assume without loss of generality that $g(\underline{Y})$ is monotone increasing.

The proposed method obtains set P_3^* by examining 2^n possible elements in numerical order [L1]; for example, in two-dimensional case, (0,0)->(1,0)->(0.1)->(1,1). The method begins with $\underline{Y}$ = (0,...,0) and ends with $\underline{Y}$ = (1,...,1). Let $\underline{Y}$ denote a vector that is currently examined, and let $\underline{Y}^p=(Y_1^p,...,Y_n^p)$ be an element of set P_3^* among the vectors that have been examined.

Step 0: Let I_S be $C_{1S}P$ and let P_3^* be empty.

Step 1: Calculate $g(\underline{Y})$ and check whether $g(\underline{Y}) > 0$.

1) If $g(\underline{Y}) \leq 0$, then calculate $g(\underline{Y})$ for the next vector.

2) Otherwise, subtract $g(\underline{Y})$ from I_S and go to Step 2.

Step 2: Compare $\underline{Y}$ with all vector $\underline{Y}^p$ in P_3^*.

1) If $\underline{Y} > \underline{Y}^p$ for some $\underline{Y}^p$, then let $\underline{Y}$ be the next vector and go to Step 1.

2) Otherwise, let $\underline{Y}$ be an element of set P_3^* and let $\underline{Y}$ be the next vector. Go to Step 1.

Through calculations described above, the set P_3^* and the optimal value of I_S can be obtained at the same time.

5.3.4 Optimal Boolean Structure of Identical Sensors

In this section, we consider the cases where some sensors are identical, where the optimal structure $f^*(\underline{Y})$ can be simplified.

We first assume that all the sensors are identical. The same theorem as the theorem of section 3.3.1 in CHAPTER 3 is obtained.

THEOREM :

Let q_1 be the FD probability and let q_2 be the FS probability of the sensor. Assume n identical sensors.

1) If $q_1 + q_2 < 1$.

a) it is optimal not to use any safety monitoring system , if $k \geq n$,

b) the safety monitoring system which is always generating the system alarm is optimal, if $k < 0$,

c) k*-out-of-n:G structure is optimal, otherwise.

2) If $q_1 + q_2 = 1$,

a) it is optimal not to use any safety monitoring system, if $C_{2S}(1-P) \geq C_{1S}P$,

b) the safety monitoring system which is always generating the system alarm is optimal, if $C_{2S}(1-P) < C_{1S}P$.

3) If $q_1 + q_2 > 1$,

a) it is optimal not to use any safety monitoring system, if $k \leq 0$,

b) the safety monitoring system which is generating the system alarm is optimal, if $k > n$,

c) k**-out-of-n:F structure is optimal, otherwise.

Notes:

1.
$$k = \frac{\ln\frac{C_{2S}(1-P)}{C_{1S}P} + n\cdot\ln\frac{1-q_1}{q_1}}{\ln\frac{(1-q_1)(1-q_1)}{q_1 q_2}}, \qquad (23)$$

2. $k^* = \mathrm{INT}[k]$,

3. $k^{**} = \mathrm{INT}[n-k]$.

Proof :

Since all the sensors are identical, the switching function

$g(\underline{Y})$ is modified into

$$\bar{g}(m) = C_{1S}P(1-q_1)^m q_1^{n-m} - C_{2S}(1-P)q_2^m(1-q_2)^{n-m}, \tag{24}$$

where

$$m = \sum_{i=1}^{n} Y_i \quad ; \text{ number of 1's in } \underline{Y}.$$

Factoring $C_{1S}P(1-q_1)^m q_1^{n-m}$ out of the right hand side of eq. (24), we have

$$\bar{g}(m) = C_{1S}P(1-q_1)^m q_1^{n-m}\{1-h(m)\}, \tag{25}$$

where

$$h(m) = \frac{C_{2S}(1-P)}{C_{1S}P}\left(\frac{1-q_2}{q_1}\right)^n\left\{\frac{q_1q_2}{(1-q_1)(1-q_2)}\right\}^m. \tag{26}$$

Eq. (25) shows that $\bar{g}(m) > 0 \Leftrightarrow h(m) < 1$.

Here the function h(m) has the following property:

P1) h(m) is decreasing with respect to m, if $q_1 + q_2 < 1$,

P2) h(m) is increasing with respect to m, if $q_1 + q_2 > 1$,

P3) h(m) is constant, if $q_1 + q_2 = 1$.

Consider the unique number k such that $h(k) = 1$; the explicit expression of k is given by eq. (23) when $q_1 + q_2 \neq 1$. If $q_1 + q_2 < 1$, then according to P1), $h(m) < 1$ for any $m > k$. Assume that $k < 0$. Then the optimal safety monitoring system always generates the system alarm. This suggests that the plant is too dangerous to operate. Assume $k \geq n$. Then the optimal system is always nullified. For other k, the optimal safety monitoring system is k*-out-of-n:G structure. If $q_1 + q_2 > 1$, then $h(m) < 1$ for any $m < k$, according to P2). The theorem can be proven similarly to the case of $q_1 + q_2 < 1$. Consider finally the case of $q_1 + q_2 = 1$. Then $h(m) = C_{2S}(1-P)/C_{1S}P$. If $C_{2S}(1-P) \geq C_{1S}P$, then $g(m) \leq 0$ for any m. The optimal safety monitoring

system is always nullified in the plant in this case. If $C_{2S}(1-P) < C_{1S}P$, then $g(m) > 0$ for any m. The optimal system always generates the system alarm.

Q.E.D.

In cases 1)-b), 2)-b), and 3)-b), the inadvertent plant state is too dangerous and it is optimal not to activate the plant. In cases 1)-a), 2)-a), and 3)-a), the safety monitoring system is too poor in reliability to be used as a protective system.

Let us consider the case where n_i sensors are available for sensor i. The switching function $g(\underline{Y})$ is modified as:

$$\bar{g}(\underline{m}) = C_{1S}P\{ \prod_{i=1}^{n} (1-q_{1i})^{m_i} q_{1i}^{n_i-m_i} \} - C_{2S}(1-P)\{ \prod_{i=1}^{n} q_{2i}^{m_i} (1-q_{2i})^{n_i-m_i} \}, \quad (27)$$

where m_i : number of sensor i's yielding the sensor alarm,

$\underline{m}$: $(m_1,\ldots,m_n)$.

From eqs. (7) and (27), the s-expected total loss I_S is

$$I_S = C_{1S}P - \sum_{\underline{m}} f(\underline{m})\bar{g}(\underline{m})\{ \prod_{i=1}^{n} \binom{n_i}{m_i} \}. \quad (28)$$

The product of the second term on the right hand side of eq. (28) means the number of vector $\underline{Y}$ which has the same value of $\bar{g}(\underline{m})$. By this modification, the number of iterations in the proposed method can be reduced to $\prod_{i=1}^{n} (m_i+1)$. Vector $\underline{m}$ of the set P_3* in this case indicates an AND combination of m_i-out-of-n_i:G or m_i-out-of-n_i:F structures of sensor i's. Thus, the optimal structure becomes an OR combination of AND combinations of m_i-out-of-n_i:G

or m_i-out-of-n_i:F structures.

5.4 ILLUSTRATIVE EXAMPLE

EXAMPLE 1 :

Consider the optimal structure composed of sensor 1 and sensor 2. The number of all the Boolean structures is ${}_2 2^2 = 16$. Assume the values of parameters in Table 5.2. Table 5.3 shows the value of the switching function for each sensor state.

Thus, the set P_1^* and the minimum of I_S are:

$P_1^* = \{ (1,0) \}$,

$I_S = 36$.

The simple form of the optimal structure is

$f^*(\underline{Y}) = Y_1$.

The optimal structure is a single-sensor system composed of sensor 1. This example shows that safety monitoring system composed of two sensors are not necessarily better than a single-sensor system: this is a specific characteristic of the systems composed of non-identical components.

EXAMPLE 2 :

Consider the optimal structure composed of three kinds of sensors, under a constraint of the investment cost. The problem is formulated as:

$$\underset{n_1,n_2,n_3}{\text{Minimize:}} \quad I_S(n_1,n_2,n_3),$$

$$\text{subject to:} \quad \sum_{i=1}^{3} c_{si} n_i \leq C_{SO},$$

$$n_i \leq n_{io},$$

Table 5.2 Values of q_{1i}, q_{2i}, C_{1S}, C_{2S}, and P

i	q_{1i}	q_{2i}	C_{1S}	C_{2S}	P
1	0.001	0.002	10000	100	0.01
2	0.003	0.004			

Table 5.3 Values of the switching function $g(\underline{Y})$

Y_1	Y_2	$g(\underline{Y})$		
0	0	$C_{1S}Pq_{11}q_{12} - C_{2S}(1-P)(1-q_{21})(1-q_{22})$	=	-98.406
1	0	$C_{1S}P(1-q_{11})q_{12} - C_{2S}(1-P)q_{21}(1-q_{22})$	=	0.102
0	1	$C_{1S}Pq_{11}(1-q_{12}) - C_{2S}(1-P)(1-q_{21})q_{22}$	=	-0.296
1	1	$C_{1S}P(1-q_{11})(1-q_{12}) - C_{2S}(1-P)q_{21}q_{22}$	=	99.600

Table 5.4 Values of q_{1i}, q_{2i}, n_{io}, c_{si}, C_{SO}, C_{1S}, C_{2S}, & P

i	q_{1i}	q_{2i}	n_{io}	c_{si}
1	0.10	0.30	5	10
2	0.05	0.10	5	20
3	0.08	0.30	5	15

C_{SO} = 100 C_{1S} = 10000 C_{2S} = 100 P = 0.2

where n_i : number of sensors of type i,

n_{io}: upper bound of n_i.

The physical condition, space or weight, places a restriction on the number of available sensors. Both the number of sensors of each type and the optimal structure are to be determined.

The objective function I_S is monotone decreasing with respect to n_1, n_2, and n_3, because more sensors become available as n_1, n_2, or n_3 gets larger. Thus, the problem can be solved by the Lawler and Bell's method [M1,S1]. Assume the data shown in Table 5.4. The number of sensors and the set P_1^* are obtained as:

$(n_1,n_2,n_3) = (0,5,0)$, $P_1^* = \{ (0,3,0) \}$.

The optimal structure is 3-out-of-5:G structure composed of sensors of type 2. The minimal s-expected total loss I_S^* is:

$I_S^* = 3.001$.

CHAPTER 6

OPTIMAL BOOLEAN STRUCTURE

OF

MULTI-PLANT-STATE MONITORING SYSTEMS

6.1 INTRODUCTION

We consider a safety monitoring system which supervises several plant states such as pressure, temperature, etc., again. In this chapter the safety monitoring system generates the system alarm based on the output of these sensors of different types, while based on the output of channels in CHAPTER 4. Further, we assume that several kinds of sensors are available for monitoring each plant state. The result of CHAPTER 5 is extended to the case where the plant to be monitored has many plant states.

The optimal logic structure to combine the sensors is developed here in order to minimize an expected total loss caused by the FD and FS failures of the system. A simple rule to determine the optimal structure among all the Boolean structures is obtained in section 6.3.1. Some properties of the optimal structure are shown, and then the same development as CHAPTER 5 follows in section 6.3.2. An illustrative example considers a three-plant-state monitoring system.

6.2 PROBLEM STATEMENT

6.2.1 Assumptions

1 The safety monitoring system is composed of N types of sensors.

2 N_i sensors of type i monitor plant state i.

3 Sensors fail s-independently.

4 Failures of sensors monitoring plant state i is s-independent of the other plant states, although those are s-dependent on plant state i.

5 Plant states malfunction s-independently.

6.2.2 Notation

X_i binary indicator variable for plant state i

$$X_i = \begin{cases} 1, & \text{if plant state i is abnormal,} \\ 0, & \text{otherwise.} \end{cases}$$

$\underline{X}$ plant state vector: $(X_1,\ldots,X_N)$

$\underline{X}(i)$ $(X_1,\ldots,X_{i-1},X_{i+1},\ldots,X_N)$

$a_i:\underline{X}(i)$ $(X_1,\ldots,X_{i-1},a,X_{i+1},\ldots,X_N)$

Y_{ij} binary indicator variable for sensor j of type i

$$Y_{ij} = \begin{cases} 1, & \text{if sensor j of type i is generating the sensor alarm,} \\ 0, & \text{otherwise.} \end{cases}$$

$\overline{Y}_{ij}$ negation of Y_{ij}; $= 1-Y_{ij}$

$\underline{Y}_i$ $(Y_{i1},\ldots,Y_{iN_i})$

$\underline{Y}_i(j)$ $(Y_{i1},\ldots,Y_{ij-1},Y_{ij+1},\ldots,Y_{iN_i})$

$a_{ij}:\underline{Y}_i(j)$ $(Y_{i1},\ldots,Y_{ij-1},a,Y_{ij+1},\ldots,Y_{iN_i})$

$\underline{Y}$ $(\underline{Y}_1,\ldots,\underline{Y}_N)$

$\underline{Y}(ij)$ $(\underline{Y}_1,\ldots,\underline{Y}_{i-1},\underline{Y}_i(j),\underline{Y}_{i+1},\ldots,\underline{Y}_N)$

$a_{ij}:\underline{Y}(ij)$ $(\underline{Y}_1,\ldots,\underline{Y}_{i-1},a_{ij}:\underline{Y}_i(j),\underline{Y}_{i+1},\ldots,\underline{Y}_N)$

$f(\underline{Y})$ structure function of the safety monitoring system

$$f(\underline{Y}) = \begin{cases} 1, & \text{if the safety monitoring system is generating the system alarm,} \\ 0, & \text{otherwise.} \end{cases}$$

$C_1(\underline{X})$ FD loss: loss caused when the safety monitoring system does not generate the system alarm under plant state $\underline{X}$

$C_2(\underline{X})$ FS loss: loss caused when the safety monitoring system generates the system alarm under the plant state $\underline{X}$

I_S s-expected total loss caused by the failures of the safety monitoring system

P_i $\Pr\{X_i=1\}$

q_{1ij} conditional FD probability of sensor j of type i: $\Pr\{Y_{ij}=0 \mid X_i=1\}$

q_{2ij} conditional FS probability of sensor j of type i: $\Pr\{Y_{ij}=1 \mid X_i=0\}$

k-out-of-n:G safety monitoring system which yields the system alarm if and only if k or more of its n sensors generate the sensor alarms. For $k \geq n+1$, it implies that the safety monitoring system is nullified. For $k \leq 0$, it implies that the safety monitoring system always generates the system alarm.

k-out-of-n:F safety monitoring system which yields the system alarm if and only if k or more its n sensors do not generate the sensor alarms. For $k \geq n+1$, it implies that the safety monitoring system is nullified. For $k \leq 0$, it implies that the safety monitoring system always generates the system alarm,

The problem is to obtain the optimal Boolean structure that minimizes an s-expected total loss caused by the failures of the safety monitoring system.

6.3 PROBLEM SOLUTION

6.3.1 Opitmal Boolean Structure of Multi-Plant-State Monitoring Systems

The s-expected total loss I_S is a sum of losses over all the plant states and the output states of sensors:

$$I_S = \sum_{\underline{X}} \sum_{\underline{Y}} [\, C_1(\underline{X})\{1-f(\underline{Y})\} + C_2(\underline{X})f(\underline{Y}) \,]\Pr\{\underline{X}\}\Pr\{\underline{Y}|\underline{X}\}. \quad (1)$$

The terms $C_1(\underline{X})\{1-f(\underline{Y})\}$ and $C_2(\underline{X})\{1-f(\underline{Y})\}$ represent the FD loss and the FS loss, respectively. Since $\Sigma_{\underline{Y}} \Pr\{\underline{Y}|\underline{X}\} = 1$, I_S is expressed as:

$$I_S = \sum_{\underline{X}} C_1(\underline{X})\Pr\{\underline{X}\} - \sum_{\underline{X}} \sum_{\underline{Y}} \{C_1(\underline{X})-C_2(\underline{X})\}\Pr\{\underline{X}\}\Pr\{\underline{Y}|\underline{X}\}. \quad (2)$$

Define $G(\underline{Y})$ as:

$$G(\underline{Y}) = \sum_{\underline{X}} \{C_1(\underline{X})-C_2(\underline{X})\}\Pr\{\underline{X}\}\Pr\{\underline{Y}|\underline{X}\}. \quad (3)$$

Then,

$$I_S = \sum_{\underline{X}} C_1(\underline{X})\Pr\{\underline{X}\} - \sum_{\underline{Y}} G(\underline{Y})f(\underline{Y}). \quad (4)$$

The first summation in eq. (4) means the loss caused in the plant without the safety monitoring system, while the second summation means the gain from implementing the safety monitoring system to the plant. If we set $f(\underline{Y}) = 1$ for any $\underline{Y}$ satisfying $G(\underline{Y}) > 0$, then I_S attains its minimum. The optimal logic structure $f^*(\underline{Y})$ is:

$$f^*(\underline{Y}) = \begin{cases} 1, & \text{if } G(\underline{Y}) > 0, \\ 0, & \text{otherwise.} \end{cases} \quad (5)$$

The function $G(\underline{Y})$ is called the switching function of the optimal

safety monitoring system. This structure is optimal among all the Boolean structures. The optimal $f^*(\underline{Y})$ can be expressed as:

$$f^*(\underline{Y}) = \sum_{\underline{Z}\in P} \prod_{i=1}^{N} \{ \prod_{j=1}^{N_i} Y_{ij}(Z_{ij}) \}, \tag{6}$$

where

$$P = \{ \underline{Y} \mid G(\underline{Y}) > 0 \}, \tag{7}$$

$$Y_{ij}(Z_{ij}) = \begin{cases} Y_{ij}, & \text{if } Z_{ij} = 1, \\ \overline{Y}_{ij}, & \text{otherwise.} \end{cases} \tag{8}$$

Eq. (5) shows that set P is the set of path vectors of the optimal logic structure $f^*(\underline{Y})$.

6.3.2 Properties of Optimal Boolean Structure

The switching function $G(\underline{Y})$ has the following property.

PROPERTY :

On the assumptions 1-5, these two properties hold:

(P1) If $q_{1ij} + q_{2ij} \leq 1$ and $G(0_{ij}:\underline{Y}(ij)) > 0$, then $G(1_{ij}:\underline{Y}(ij)) > 0$.

(P2) If $q_{1ij} + q_{2ij} > 1$ and $G(1_{ij}:\underline{Y}(ij)) > 0$, then $G(0_{ij}:\underline{Y}(ij)) > 0$.

Proof :

From the assumptions 3-5 and eq. (3), $G(0_{ij}:\underline{Y}(ij))$ and $G(1_{ij}:\underline{Y}(ij))$ can be written as:

$$G(0_{ij}:\underline{Y}(ij)) = C_1 P_i q_{1ij} \Pr\{\underline{Y}_i(j) \mid X_i=1\} + C_2(1-P_i)(1-q_{2ij})\Pr\{\underline{Y}_i(j) \mid X_i=0\}, \tag{9}$$

$$G(1_{ij}:\underline{Y}(ij)) = C_1 P_i (1-q_{1ij})\Pr\{\underline{Y}_i(j) \mid X_i=1\} + C_2(1-P_i)q_{2ij}\Pr\{\underline{Y}_i(j) \mid X_i=0\}, \tag{10}$$

where

$$C_1 = \sum_{\underline{X}=(1_i:\underline{X}(i))} \{C_1(\underline{X})-C_2(\underline{X})\}Pr\{\underline{X}(i)\}Pr\{\underline{Y}(i)|\underline{X}(i)\}, \quad (11)$$

$$C_2 = \sum_{\underline{X}=(0_i:\underline{X}(i))} \{C_1(\underline{X})-C_2(\underline{X})\}Pr\{\underline{X}(i)\}Pr\{\underline{Y}(i)|\underline{X}(i)\}, \quad (12)$$

$$Pr\{\underline{X}(i)\} = \prod_{j\neq i} \{ X_jP_j + (1-X_j)(1-P_j) \}, \quad (13)$$

$$Pr\{\underline{Y}(i)|\underline{X}(i)\} = \prod_{j\neq i} [\prod_{h=1}^{N_j} (X_j\{Y_{jh}(1-q_{1jh})+(1-Y_{jh})q_{1jh}\} + (1-X_j)\{Y_{jh}q_{2jh}+(1-Y_{jh})(1-q_{2jh})\})], \quad (14)$$

$$Pr\{\underline{Y}_i(j)|X_i=1\} = \prod_{h\neq j} \{ Y_{ih}(1-q_{1ih}) + (1-Y_{ih})q_{1ih} \}, \quad (15)$$

$$Pr\{\underline{Y}_i(j)|X_i=0\} = \prod_{h\neq j} \{ Y_{ih}q_{2ih} + (1-Y_{ih})(1-q_{2ih}) \}, \quad (16)$$

Suppose a natural assumption on $C_1(\underline{X})$ and $C_2(\underline{X})$: $C_1(\underline{X})$ is monotone increasing with respect to $\underline{X}$, while $C_2(\underline{X})$ is monotone decreasing with respect to $\underline{X}$. Then, from eqs. (11) and (12), $C_1 > C_2$. Let us prove the property (P1) first. The two cases are possible;

Case 1: $C_1 > 0$ and $C_2 \geq 0$. Case 2: $C_1 > 0$ and $C_2 < 0$.

In case 1, it is obvious that $G(1_{ij}:\underline{Y}(ij)) > 0$ because $0 < P_i < 1$, $0 < q_{1ij} < 1$, $0 < q_{2ij} < 1$, $Pr\{\underline{Y}_i(j)|X_i=1\} > 0$, and $Pr\{\underline{Y}_i(j)|X_i=0\} > 0$ in eq. (10). In case 2, the same proof as that in section 5.3.2 of CHAPTER 5 can be applied. The property (P2) can be proven in a similar way.

Q.E.D.

The function $G(\underline{Y})$ has the same property as that of the function $g(\underline{Y})$ in CHAPTER 5. Replacing $g(\underline{Y})$ by $G(\underline{Y})$, the same development holds for this case.

Now we consider Case 3 as a general case. Let $\underline{Y}_1$ denote the vector of indicator variables for sensor j of type i such that

$q_{1ij} + q_{2ij} \leq 1$. Let $\underline{Y}_2$ denote the vector of Y_{ij} such that $q_{1ij} + q_{2ij} > 1$. Then, the property proven here shows that the optimal structure function $f^*(\underline{Y}_1, \underline{Y}_2)$ is monotone increasing with respect to $\underline{Y}_1$, while it is monotone decreasing with respect to $\underline{Y}_2$. That is,

$$\underline{Y}_1 > \underline{Y}_1' \quad ====> \quad f^*(\underline{Y}_1, \underline{Y}_2) \geq f^*(\underline{Y}_1', \underline{Y}_2),$$

$$\underline{Y}_2 > \underline{Y}_2' \quad ====> \quad f^*(\underline{Y}_1, \underline{Y}_2') \geq f^*(\underline{Y}_1, \underline{Y}_2).$$

The set of minimal path vectors can be defined as:

$$P^* = \{ (\underline{Y}_1, \underline{Y}_2) \mid G(\underline{Y}_1, \underline{Y}_2) > 0 \text{ and; if } \underline{Y}_1 > \underline{Y}_1', \text{ then } G(\underline{Y}_1', \underline{Y}_2) \leq 0 \text{ and; if } \underline{Y}_2 < \underline{Y}_2', \text{ then } G(\underline{Y}_1, \underline{Y}_2') \leq 0 \}. \quad (17)$$

The simple expression of the structure function $f^*(\underline{Y})$ is

$$f^*(\underline{Y}) = \coprod_{(\underline{Z}_1, \underline{Z}_2) \in P^*} \{ (\prod_{(ij) \in C_1(\underline{Z}_1)} Y_{ij}) (\prod_{(ij) \in C_0(\underline{Z}_2)} \overline{Y}_{ij}) \}, \quad (18)$$

where

$$C_1(\underline{Z}) = \{ (ij) \mid Z_{ij} = 1 \}, \quad (19)$$

$$C_0(\underline{Z}) = \{ (ij) \mid Z_{ij} = 0 \}. \quad (20)$$

The minimal path vectors of $f^*(\underline{Y})$ can be obtained by the same systematic method as in section 5.3.3 of CHAPTER 5 with $G(\underline{Y})$ in place of $g(\underline{Y})$.

If the safety monitoring system supervises only one plant state, then $C_1(X_1=0) = 0$ and $C_2(X_1=1) = 0$ because the normal operation of the safety monitoring system does not cause any loss. In this case, the function $G(\underline{Y})$ has the same form as that of $g(\underline{Y})$. Thus, $G(\underline{Y})$ is a natural extension of $g(\underline{Y})$.

Consider the case where n_{ij} sensors are available for sensor j of type i. Then, the function $G(\underline{Y})$ is modified by assumptions 3-5 as follows:

$$\overline{G}(\underline{m}) = \sum_{\underline{X}} \{C_1(\underline{X}) - C_2(\underline{X})\} \Pr\{\underline{X}\} \Pr\{\underline{m} \mid \underline{X}\}, \quad (21)$$

where

m_{ij} : number of sensor j of type i which is yielding the sensor alarm,

$\underline{m}$: $(m_{11},\ldots,m_{1N_1},\ldots,m_{N1},\ldots,m_{NN_N})$

$$\Pr\{\underline{m}|\underline{X}\} = \prod_{i=1}^{N} [\, X_i \{ \prod_{j=1}^{N_i} q_{1ij}^{m_{ij}} (1-q_{1ij})^{n_{ij}-m_{ij}} \} + (1-X_i)\{ \prod_{j=1}^{N_i} q_{2ij}^{m_{ij}} (1-q_{2ij})^{n_{ij}-m_{ij}} \} \,]. \quad (22)$$

The s-expected total loss I_S is:

$$I_S = \sum_{\underline{X}} C_1(\underline{X}) \Pr\{\underline{X}\} - \sum_{\underline{m}} [\prod_{i=1}^{N} \{ \prod_{j=1}^{N_i} \binom{n_{ij}}{m_{ij}} \}] \bar{G}(\underline{m}) f(\underline{m}). \quad (23)$$

Vector $\underline{m}$ in the set of minimal path vectors reduces to an AND combination of m_{ij}-out-of-n_{ij}:G or m_{ij}-out-of-n_{ij}:F structures. Thus, the optimal structure $f^*(\underline{Y})$ in this case results in an OR combination of AND combinations of m_{ij}-out-of-n_{ij}:G or m_{ij}-out-of-n_{ij}:F structures.

6.4 ILLUSTRATIVE EXAMPLE

Consider a safety monitoring system, which supervises flow X_1, pressure X_2, and temperature X_3. If {loss-of-flow} OR {high-pressure AND high-temperature} take place in the plant, then the plant suffers a considerable loss. There are 8 possible combinations of the plant parameters X_1, X_2, X_3. FD and FS losses over all the plant states are shown in Table 6.1, where X_1 = 1 indicates that {loss-of-flow} takes place in the plant. Similarly, X_2 = 1 and X_3 = 1 indicate the occurence of {high-pressure} and {high-temperature}.

Table 6.2 shows failure probabilities of sensor i and plant

Table 6.1 Losses over each plant state

X_1	X_2	X_3	$C_1(\underline{X})$	$C_2(\underline{X})$
0	0	0	0	100
1	0	0	2000	0
0	1	0	0	50
1	1	0	7000	0
0	0	1	0	80
1	0	1	8000	0
0	1	1	5000	0
1	1	1	10000	0

Table 6.2 Values of q_{1il}, q_{2il}, & P_i

i	q_{1il}	q_{2il}	P_i
1	0.03	0.006	0.02
2	0.01	0.008	0.03
3	0.05	0.010	0.01

Table 6.3 Values of the switching function $G(\underline{m})$

m_1	m_2	m_3	$G(\underline{m})$	m_1	m_2	m_3	$G(\underline{m})$	m_1	m_2	m_3	$G(\underline{m})$	m_1	m_2	m_3	$G(\underline{m})$
0	0	0	-59.058	0	0	1	-1.793	0	0	2	-0.085	0	0	3	-0.442
1	0	0	-11.233	1	0	1	-0.341	1	0	2	-0.016	1	0	3	-0.078
2	**0**	**0**	1.736	2	0	1	0.053	2	0	2	0.014	2	0	3	0.083
3	0	0	26.473	3	0	1	0.810	3	0	2	0.157	3	0	3	0.946
0	1	0	-15.407	0	1	1	-0.468	0	1	2	-0.022	0	1	3	-0.110
1	1	0	-2.930	1	1	1	-0.089	1	1	2	-0.004	1	1	3	-0.020
2	1	0	0.453	2	1	1	0.014	2	1	2	0.004	2	1	3	0.022
3	1	0	6.907	3	1	1	0.211	3	1	2	0.041	3	1	3	0.247
0	2	0	-1.374	0	2	1	-0.041	**0**	**2**	**2**	0.003	0	2	3	0.021
1	2	0	-0.261	1	2	1	-0.008	1	2	2	0.0006	1	2	3	0.004
2	2	0	0.490	2	2	1	0.002	2	2	2	0.0004	2	2	3	0.002
3	2	0	0.709	3	2	1	0.022	3	2	2	0.004	3	2	3	0.023
0	3	0	-1.177	0	3	1	-0.027	0	3	2	0.160	0	3	3	1.015
1	3	0	-0.215	1	3	1	-0.005	1	3	2	0.031	1	3	3	0.195
2	3	0	0.319	2	3	1	0.010	2	3	2	0.003	2	3	3	0.017
3	3	0	3.590	3	3	1	0.109	3	3	2	0.008	3	3	3	0.046

state i. Assume that 3 identical sensors are available for each type i. In this case, the optimal structure can be determined by $\bar{G}(\underline{m})$ more easily than $G(\underline{Y})$. In Table 6.3, $G(\underline{m})$ indicates values of the modified switching function $\bar{G}(\underline{m})$ multiplied by number the of equivalent sensor states $\underline{Y}$. Then the minimum of I_S turns out to be: $I_S^* = 1.141$. The set of P*' of the optimal structure is:

$$P^{*\prime} = \{ (2,0,0),(0,2,2) \}.$$

The optimal safety monitoring system yields the system alarm and activates the corresponding safety system, if {2 or more sensors of type 1} OR [{2 or more sensors of type 2} AND {2 or more sensors of type 3}] yield the sensor alarms.

CHAPTER 7

OPTIMAL BOOLEAN STRUCTURE

OF

STATISTICALLY-DEPENDENT-PLANT-STATE MONITORING SYSTEMS

7.1 INTRODUCTION

In CHAPTER 6, we assumed that plant states malfunction s-independently. However, the s-independence of failures does not hold in practice. Common-mode failures such as a flood cause all supposedly redundant components to fail simultaneously. As another example, consider the structure in which components share the load. Then, the failure of one component results in increased load on each of the remaining components; the failure of a component contributes to the failure of the remaining components. Thus, in this chapter we consider the safety monitoring system, supervising s-dependent plant states.

The plant is assumed to suffer losses when any plant state becomes abnormal. The optimal logic structure is determined by a switching function in section 7.3.1. We propose a clssification of sensors into two classes: "positively reliable" and "negatively reliable", in the following section. The monotone property of the optimal structure is proven with these two terms. Section 7.3.4 deals with the case where several sensors are

identical. The optimal logic structure is also analytically obtained when all the sensors are identical. An illustrative example in section 7.4 considers a glass-lined reactor, where three s-dependent phenomena are supervised by the safety moniotoring system.

7.2 PROBLEM STATEMENT

7.2.1 Assumptions

1 The safety monitoring system is composed of N types of sensors.

2 Sensors of type i monitor plant state i.

3 Each sensor is either generating the sensor alarm or not.

4 Failures of sensors of type i are s-independent of the other plant states except i, although they are s-dependent on plant state i.

5 The plant suffers losses when any plant state becomes abnormal.

7.2.2 Notation

X_i binary indicator variable for plant state i

$$X_i = \begin{cases} 1, & \text{if plant state i is abnormal,} \\ 0, & \text{otherwise.} \end{cases}$$

$\underline{X}$ plant state vector : $(X_1,\ldots,X_N)$

$\underline{X}(i)$ $(X_1,\ldots,X_{i-1},X_{i+1},\ldots,X_N)$

Y_{ij} binary indicator variable for sensor j of type i

$$Y_{ij} = \begin{cases} 1, & \text{if sensor j of type i is generating the sensor alarm,} \\ 0, & \text{otherwise.} \end{cases}$$

$\bar{Y}_{ij}$ negation of Y_{ij}; $= 1 - Y_{ij}$

$\underline{Y}$ $(Y_{11},\ldots,Y_{1N_1},\ldots,Y_{N1},\ldots,Y_{NN_N})$

$\underline{Y}(ij)$ $(Y_{11},\ldots,Y_{1N_1},\ldots,Y_{ij-1},Y_{ij+1},\ldots,Y_{N1},\ldots,Y_{NN_N})$

$a_{ij}:\underline{Y}(ij)$ $(Y_{11},\ldots,Y_{1N_1},\ldots,Y_{ij-1},a,Y_{ij+1},\ldots,Y_{N1},\ldots,Y_{NN_N})$

$f(\underline{Y})$ binary indicator variable for the safety monitoring system

$$f(\underline{Y}) = \begin{cases} 1, & \text{if the safety monitoring system is generating the system alarm,} \\ 0, & \text{otherwise.} \end{cases}$$

$C_1(\underline{X})$ FD loss: loss caused when the safety monitoring system fails to generate the system alarm under plant state $\underline{X}$

$C_2(\underline{X})$ FS loss: loss caused when the safety monitoring system generates the system alarm under plant state $\underline{X}$

I_S s-expected total loss caused by the failures of the safety monitoring system

q_{1ij} conditional FD probability of sensor j of type i: $\Pr\{Y_{ij}=0 \mid X_i=1\}$

q_{2ij} conditional FS probability of sensor j of type i: $\Pr\{Y_{ij}=1 \mid X_i=0\}$

k-out-of-n:G safety monitoring system which generates the system alarm if and only if k or more of its n sensors generate the sensor alarms. For $k \geq n+1$, it implies that the safety monitoring system is nullified. For $k \leq 0$, it implies that the safety monitoring system always generates the system alarm.

k-out-of-n:F safety monitoring system which generates the

system alarm if and only if k or more of its n sensors do not generate the sensor alarms. For $k \geq n+1$, it implies that the safety monitoring system is nullified. For $k \leq 0$, it implies that the safety monitoring system always generates the system alarm.

The problem is to obtain the optimal Boolean structure that minimizes an s-expected total loss caused by the failures of the safety monitoring system.

7.3 PROBLEM SOLUTION

7.3.1 Optimal Boolean Structure of Statistically-Dependent-Plant-State Monitoring Systems

The s-expected total loss I_S is :

$$I_S = \sum_{\underline{X}} \sum_{\underline{Y}} [C_1(\underline{X})\{1-f(\underline{Y})\}+C_2(\underline{X})f(\underline{Y})]\Pr\{\underline{X}\}\Pr\{\underline{Y}|\underline{X}\}. \quad (1)$$

The similar development as in section 6.3.1 of CHAPTER 6 holds:

$$I_S = \sum_{\underline{X}} C_1(\underline{X})\Pr\{\underline{X}\} - \sum_{\underline{Y}} G(\underline{Y})f(\underline{Y}), \quad (2)$$

$$G(\underline{Y}) = \sum_{\underline{X}} \{C_1(\underline{X})-C_2(\underline{X})\}\Pr\{\underline{X}\}\Pr\{\underline{Y}|\underline{X}\}. \quad (3)$$

The optimal logic structure $f^*(\underline{Y})$ is:

$$f^*(\underline{Y}) = \begin{cases} 1, & \text{if } G(\underline{Y}) > 0, \\ 0, & \text{otherwise.} \end{cases} \quad (4)$$

The optimal $f^*(\underline{Y})$ can be expressed as:

$$f^*(\underline{Y}) = \sum_{\underline{Z} \in P} \prod_{i=1}^{N} \{ \prod_{j=1}^{N_i} Y_{ij}(Z_{ij})\}, \quad (5)$$

where

$$P = \{ \underline{Y} \mid G(\underline{Y}) > 0 \}, \quad (6)$$

$$Y_{ij}(Z_{ij}) = \begin{cases} Y_{ij}, & \text{if } Z_{ij} = 1, \\ \overline{Y}_{ij}, & \text{otherwise.} \end{cases} \quad (7)$$

For the s-dependent case, the structure function can be simplified by a prime implicant algorithm [K19].

7.3.2 Definitions of "Positively Reliable" and "Negatively Reliable"

Before demonstrating the monotone property of the optimal structure, we introduce here the concepts of "positively reliable" and "negatively reliable" sensors.

Sensor j of type i is called positively reliable if the following inequality is always satisfied:

$$\Pr\{Y_{ij}=1 \mid \underline{Y}(ij), X_i=1\} \geq \Pr\{Y_{ij}=1 \mid \underline{Y}(ij), X_i=0\}. \quad (8)$$

The positively reliable sensor is equally or more likely to generate the correct alarm than it generates the false alarm. If failures of sensors are s-independent, then eq. (8) becomes

$$q_{1ij} + q_{2ij} \leq 1. \quad (9)$$

Sensor j of type i is called negatively reliable if the following inequality always holds.

$$\Pr\{Y_{ij}=1 \mid \underline{Y}(ij), X_i=1\} < \Pr\{Y_{ij}=1 \mid \underline{Y}(ij), X_i=0\}. \quad (10)$$

The negatively reliable sensor is equally or more likely to generate the false alarm than it generates the correct alarm. If sensors fail s-independently, then eq. (10) becomes

$$q_{1ij} + q_{2ij} > 1. \quad (11)$$

7.3.3 Monotone Property of Optimal Boolean Structure

The switching function $G(\underline{Y})$ also has a similar property to that in section 6.3.2 of CHAPTER 6.

PROPERTY :

On the assumptions 1-5, the following properties hold:

(P1) If sensor j of type i is positively reliable and $G(0_{ij}:\underline{Y}(ij)) > 0$, then $G(1_{ij}:\underline{Y}(ij)) > 0$.

(P2) If sensor j of type i is negatively reliable and $G(1_{ij}:\underline{Y}(ij)) > 0$, then $G(0_{ij}:\underline{Y}(ij)) > 0$.

Proof :

From eq. (3), $G(0_{ij}:\underline{Y}(ij))$ and $G(1_{ij}:\underline{Y}(ij))$ can be written as:

$$G(0_{ij}:\underline{Y}(ij)) = C_1 Pr\{Y_{ij}=0|\underline{Y}(ij),X_i=1\}+C_2 Pr\{Y_{ij}=0|\underline{Y}(ij),X_i=0\}, \quad (12)$$

$$G(1_{ij}:\underline{Y}(ij)) = C_1 Pr\{Y_{ij}=1|\underline{Y}(ij),X_i=1\}+C_2 Pr\{Y_{ij}=1|\underline{Y}(ij),X_i=0\}, \quad (13)$$

where

$$C_1 = \sum_{\underline{X}=(1_i:\underline{X}(i))} \{C_1(\underline{X})-C_2(\underline{X})\} Pr\{\underline{X},\underline{Y}(ij)\}, \quad (14)$$

$$C_2 = \sum_{\underline{X}=(0_i:\underline{X}(i))} \{C_1(\underline{X})-C_2(\underline{X})\} Pr\{\underline{X},\underline{Y}(ij)\}. \quad (15)$$

From assumption 5, the loss functions $C_1(\underline{X})$ and $C_2(\underline{X})$ are:

$$\begin{aligned} &C_1(\underline{X}) = 0 \text{ and } C_2(\underline{X}) > 0, \quad \text{for } \underline{X} = (0,\ldots,0), \\ &C_1(\underline{X}) > 0 \text{ and } C_2(\underline{X}) = 0, \quad \text{for } \underline{X} \neq (0,\ldots,0), \end{aligned} \quad (16)$$

because the plant suffers damage 1) when any plant state gets abnormal and the protective system does not work and 2) when the protective system shuts down the plant under the normal state of the plant, where all the plant states are normal. Then, eq. (14) shows that $C_1 > 0$. Let us prove the property (P1) first. Since $G(0_{ij}:\underline{Y}(ij)) > 0$ and $C_1 > 0$, the following inequality can be obtained from eq. (12):

$$C_2 > - C_1 \frac{Pr\{Y_{ij}=0|\underline{Y}(ij),X_i=1\}}{Pr\{Y_{ij}=1|\underline{Y}(ij),X_i=0\}}. \quad (17)$$

Then,

$$G(1_{ij}:\underline{Y}(ij)) > C_1 \Pr\{Y_{ij}=1|\underline{Y}(ij),X_i=1\} x$$

$$[1 - \frac{\Pr\{Y_{ij}=1|\underline{Y}(ij),X_i=0\}\Pr\{Y_{ij}=0|\underline{Y}(ij),X_i=1\}}{\Pr\{Y_{ij}=1|\underline{Y}(ij),X_i=1\}\Pr\{Y_{ij}=0|\underline{Y}(ij),X_i=0\}}]. \quad (18)$$

The assumption that sensor j of type i is positively reliable implies the inequalities:

$$\frac{\Pr\{Y_{ij}=1|\underline{Y}(ij),X_i=0\}}{\Pr\{Y_{ij}=1|\underline{Y}(ij),X_i=1\}} \leq 1, \quad (19)$$

$$\frac{\Pr\{Y_{ij}=0|\underline{Y}(ij),X_i=1\}}{\Pr\{Y_{ij}=0|\underline{Y}(ij),X_i=0\}} \leq 1. \quad (20)$$

Eqs. (18)-(20) show that $G(1_{ij}:\underline{Y}(ij)) > 0$. The property (P2) can be proven in a similar way.

Q.E.D.

According to the property, the optimal structure function $f^*(\underline{Y})$ has a monotone property which is similar to the s-independent case in CHAPTER 6.

MONOTONE PROPERTY :

The optimal structure function $f^*(\underline{Y})$ has the following properties on assumptions 1-5.

(P1) The function $f^*(\underline{Y})$ is monotone increasing with respect to the indicator variable Y_{ij} of positively reliable sensor:
$f^*(0_{ij}:\underline{Y}(ij)) \leq f^*(1_{ij}:\underline{Y}(ij))$.

(P2) The function $f^*(\underline{Y})$ is monotone decreasing with respect to the indicator variable Y_{ij} of negatively reliable sensor:
$f^*(1_{ij}:\underline{Y}(ij)) \leq f^*(0_{ij}:\underline{Y}(ij))$.

The monotone property implies that the systematic search in section 5.3.3 of CHAPTER 5 can be also applied to obtain minimal

path vectors.

7.3.4 Optimal Boolean Structure of Identical Sensors

Let us consider the case where n_{ij} sensors are available for sensor j of type i. Since the identical sensors have the same statistical characteristic, the probability that a specific set of m_{ij} sensors are issuing the sensor alarms whilst the remaining $(n_{ij}-m_{ij})$ are not doing must be the same for all sets of m_{ij} components. In this case, the function $G(\underline{Y})$ is modified into

$$\bar{G}(\underline{m}) = \sum_{\underline{X}} \{C_1(\underline{X}) - C_2(\underline{X})\}\Pr\{\underline{X}\}\Pr\{\underline{m}|\underline{X}\}, \tag{21}$$

where

m_{ij} : number of sensor j of type i which is yielding the sensor alarm,

$\underline{m}$: $(m_{11},\ldots,m_{1N_1},\ldots,m_{N1},\ldots,m_{NN_N})$.

The s-expected total loss I_S is:

$$I_S = \sum_{\underline{X}} C_1(\underline{X})\Pr\{\underline{X}\} - \sum_{\underline{m}} \left[\prod_{i=1}^{N}\left\{\prod_{j=1}^{N_i}\binom{n_{ij}}{m_{ij}}\right\}\right]\bar{G}(\underline{m})f(\underline{m}). \tag{22}$$

Then, the optimal logic structure can be more easily determined by the modified switching function $\bar{G}(\underline{m})$. Element $\underline{m}$ in the set of minimal path vectors implies an AND combination of m_{ij}-out-of-n_{ij}:G for a positively-reliable sensor and m_{ij}-out-of-n_{ij}:F for a negatively-reliable sensor. Thus, the optimal logic structure is expressed by an OR combination of AND combinations of m_{ij}-out-of-n_{ij}:G and m_{ij}-out-of-n_{ij}:F structures.

Sensors in practical applications satisfy the positively reliable condition. In this case, the safety monitoring system generates the system alarm if and only if m_{ij} or more of sensor j of type i yield the sensor alarms for all i and j.

As a special case, we consider again the safety monitoring system composed of n identical sensors, supervising a specific plant state. Since the normal operation of the safety monitoring system does not cause any loss, the loss functions $C_1(X)$ and $C_2(X)$ become:

$C_1(X=1) = C_{1S} > 0$, $\quad C_1(X=1) = 0$,

$C_1(X=0) = 0$, $\quad C_2(X=0) = C_{2S} > 0$.

According to the monotone property proven in the previous section, a similar theorem as in section 5.3.4 of CHAPTER 5 holds for this case.

THEOREM :

Assume n identical sensors. On assumptions 1-5, the optimal Boolean structure that minimizes the s-expected total loss I_S (eq. (22)) is determined as:

(1) If the sensor is positively reliable, then k*-out-of-n:G structure is optimal.

(2) If the sensor is negatively reliable, then (n-k**)-out-of-n:F structure is optimal.

Note a) k* is the minimum integer k such that $\bar{g}(k) > 0$.

b) k** is the maximum integer k such that $\bar{g}(k) > 0$.

c) $\bar{g}(k) = C_{1S}Pr\{X=1\}Pr\{m|X=1\} - C_{2S}Pr\{X=0\}Pr\{m|X=0\}$.

For the s-independent case, $\bar{g}(k)$ becomes equivalent to eq. (24) of CHAPTER 5.

7.4 ILLUSTRATIVE EXAMPLE

Consider a chemical process which chlorinates a hydrocarbon

gas in a glass-lined reactor as shown in Fig. 7.2 [K20]. The possibility of an exothermic, runaway reaction occurs whenever the Chlorine/Hydrocarbon gas ratio is too high, in which case a detonation occurs, since a source of ignition is always present. There are three unsafe phenomena: a high chlorine flow X_1, a low hydrocarbon flow X_2, and a high chlorine to hydrocarbon gas ratio X_3 in the reactor. The chlorine flow must be shut off when an unsafe state is detected by the safety monitoring system, reducing the Chlorine/Hydrocarbon ratio.

There are eight possible combinations of the plant parameters X_1, X_2, and X_3, as shown in Table 7.1. The FD loss $C_1(\underline{X})$ is caused when the safety monitoring system does not shut off the chlorine flow at the plant state $\underline{X} = (X_1, X_2, X_3)$. The zero value of $C_1(\underline{X})$ implies that no loss results at state $\underline{X} = (0,0,0)$ even if the safety monitoring system does not shut off the chlorine flow. The FS loss $C_2(\underline{X})$ indicates how much cost is caused when the chlorine is shut off at plant state $\underline{X}$. The absolute values of $C_1(\underline{X})$ and $C_2(\underline{X})$ are not always required; the ratio $C_1(\underline{X})/C_2(\underline{X}'=(0,0,0))$ are sufficient to identify the signum of the switching function $G(\underline{Y})$, reflecting a trade-off between the FS loss and the FD loss. We must ask ourselves how many FS failures are equivalent to the single FD failure at a given state of the plant. We answer for the glass-lined reactor that 100 spurious shut-downs can be traded off by one event of failing to shut down, yielding the loss values in Table 7.1.

The demand probability $\Pr\{\underline{X}\}$ denotes the likelihood of the plant state, which can be obtained from the plant operating data. The probability in the second row of Table 7.1 is zero since X_1 =

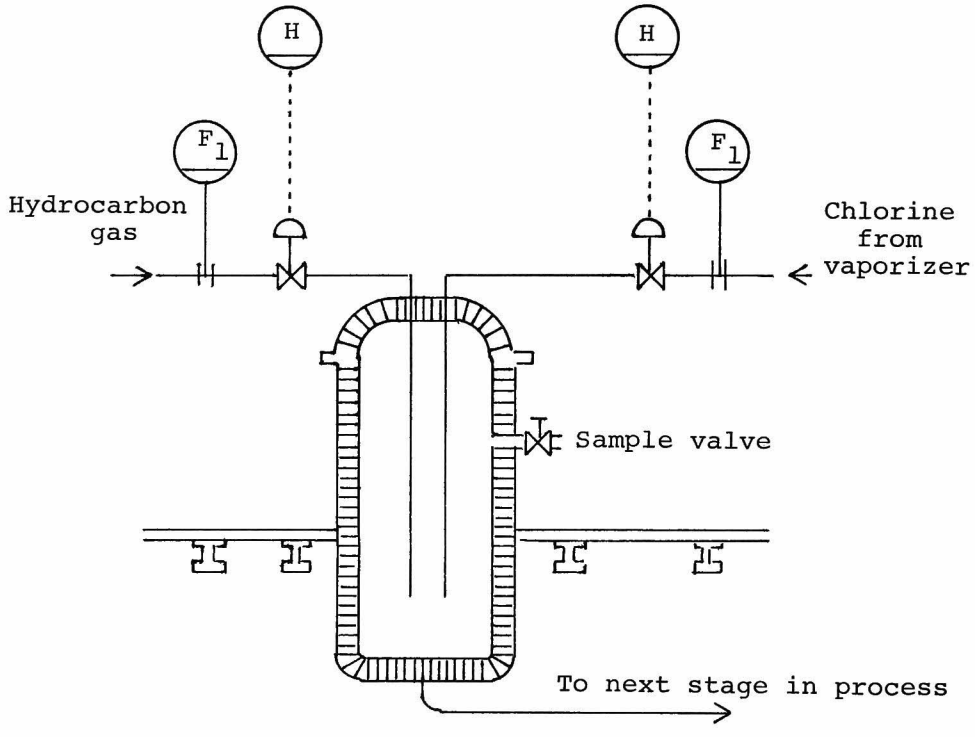

Fig. 7.1 Glass-lined reactor

Table 7.1 Values of $C_1(\underline{X})$, $C_2(\underline{X})$, and $Pr\{\underline{X}\}$

X_1	X_2	X_3	$C_1(\underline{X})$	$C_2(\underline{X})$	$Pr\{\underline{X}\}$
0	0	0	0	1	$(1-2.4\times10^{-4})(1-1.4\times10^{-5})$
0	0	1	100	0	0
0	1	0	100	0	0
0	1	1	100	0	$(1-2.4\times10^{-4})(1.4\times10^{-5})$
1	0	0	100	0	0
1	0	1	100	0	$(2.4\times10^{-4})(1-1.4\times10^{-5})$
1	1	0	100	0	0
1	1	1	100	0	$(2.4\times10^{-4})(1.4\times10^{-5})$

Table 7.2 Values of q_{1ij} and q_{2ij}

i	q_{1ij}	q_{1ij}
1	0.25	4.3×10^{-5}
2	0.25	4.3×10^{-5}
3	0.25	4.3×10^{-5}

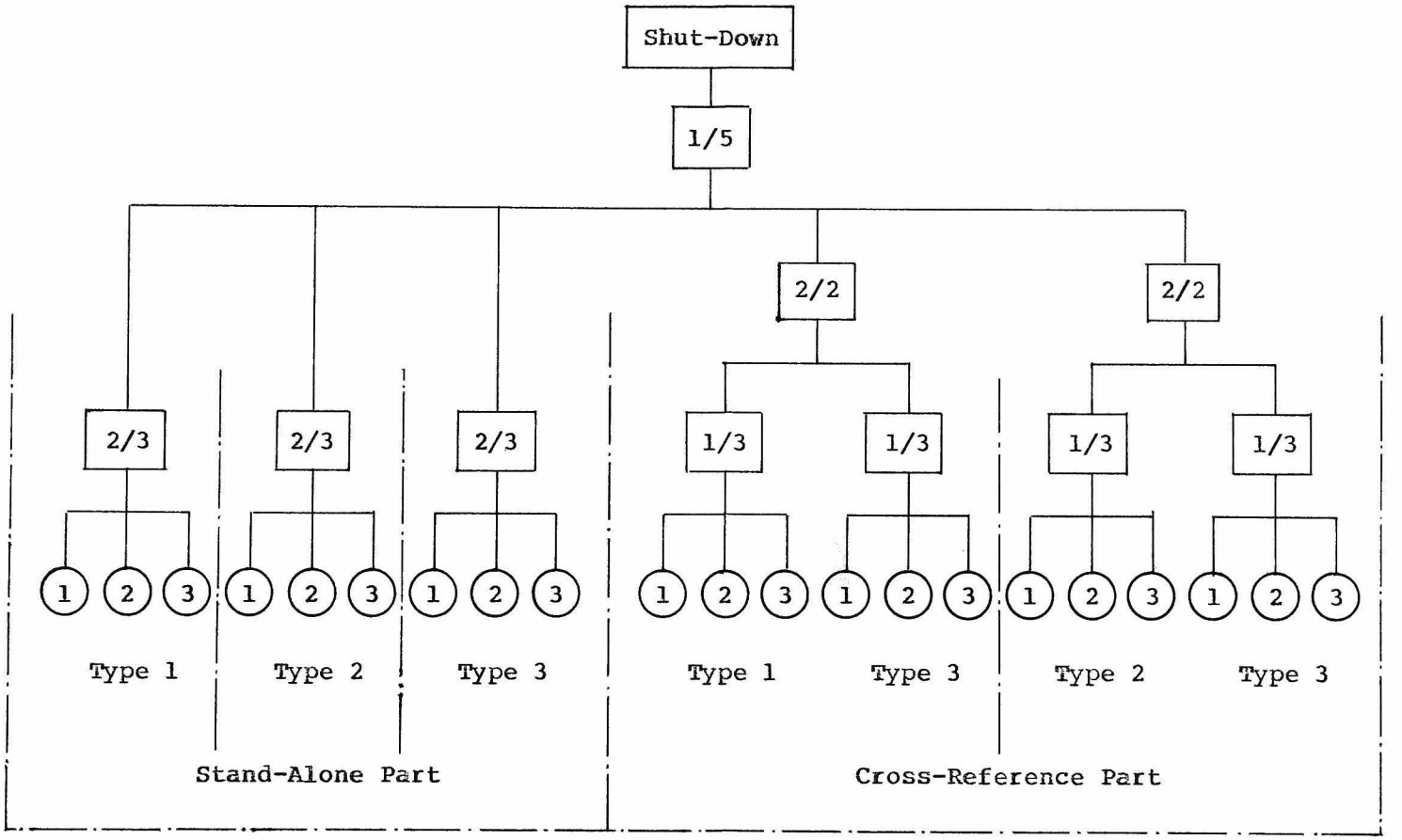

Fig. 7.2 Optimal logic structure for glass-lined reactor

0 AND $X_2 = 0$ implies $X_3 = 0$. The other zero probabilities can be interpreted similarly. Note in Table 7.1 the s-independence between X_1 and X_2, and the complete s-dependence of X_3 on X_1 or X_3.

Assume that 3 identical sensors are available for monitoring each plant state i. Table 7.2 shows the conditional FD and FS probabilities of sensors of type i. Probability $\Pr\{\underline{Y}|\underline{X}\}$ can be calculated as:

$$\Pr\{\underline{Y}|\underline{X}\} = \prod_{i=1}^{3} \prod_{j=1}^{3} [X_i\{Y_{ij}(1-q_{1ij}) + \bar{Y}_{ij}q_{1i}\} + \bar{X}_i\{Y_{ij}q_{2ij} + \bar{Y}_{ij}(1-q_{2ij})\}. \quad (21)$$

The optimal logic structure function $f^*(\underline{Y})$ is shown in Fig. 7.3. This consists of a stand-alone part and a cross-reference part. In the former, any 2-out-of-3:G majority rule over the sensors of the same type can shut down the plant. In the latter part, two 1-out-of-3:G are ANDed to generate the system alarm. We observe the following points:

The 1/3 logic of type 1 is ANDed by the 1/3 logic of type 3 in the cross-reference part. The 1/3 logic of type 1 is more FS than the 2/3 logic in the stand-alone part. This trend is compensated because the alarm signal from the 1/3 logic of type 1 is doubly checked by the alarm signal from the 1/3 logic of type 3. The abnormal plant state X_3, i.e., high gas ratio in reactor, should be detected simultaneously with the plant state X_1, i.e., high chlorine flow. The 1/3 logic structures of type 1 and 2 are not cross-referenced because plant state X_1 and X_2 occur s-independently, and such a double checking is not justified. The cross-reference of type 2 and type 3 can be interpreted similarly

to the cross-reference of types 1 and 3.

CHAPTER 8

OPTIMAL SHUT-DOWN LOGIC

OF

OVERALL PROTECTIVE SYSTEMS

8.1 INTRODUCTION

An overall protective system is composed of sensing, judging, and driving sections, as shown in Fig. 8.1. The state of the plant is monitored by the sensing section which consists of several types of sensors. If some state becomes abnormal, the corresponding sensor issues its sensor alarm. The judging section decides whether the driving section should be activated or not, examining all the signals from the sensing section, and the plant is shut down. The plant and the protective system constitute a closed-loop.

In the previous chapters, we considered the sensing section combined with the judging section as the safety monitoring system, assuming that the judging section does not fail. Here, we relax this assumption, and assume that each section has two kinds of contradictory failures: FD and FS. This chapter develops how to generate a command to the driving section, considering all failures of the three sections. The optimal shut-down logic is obtained by a switching function in section 8.3.1. A Boolean

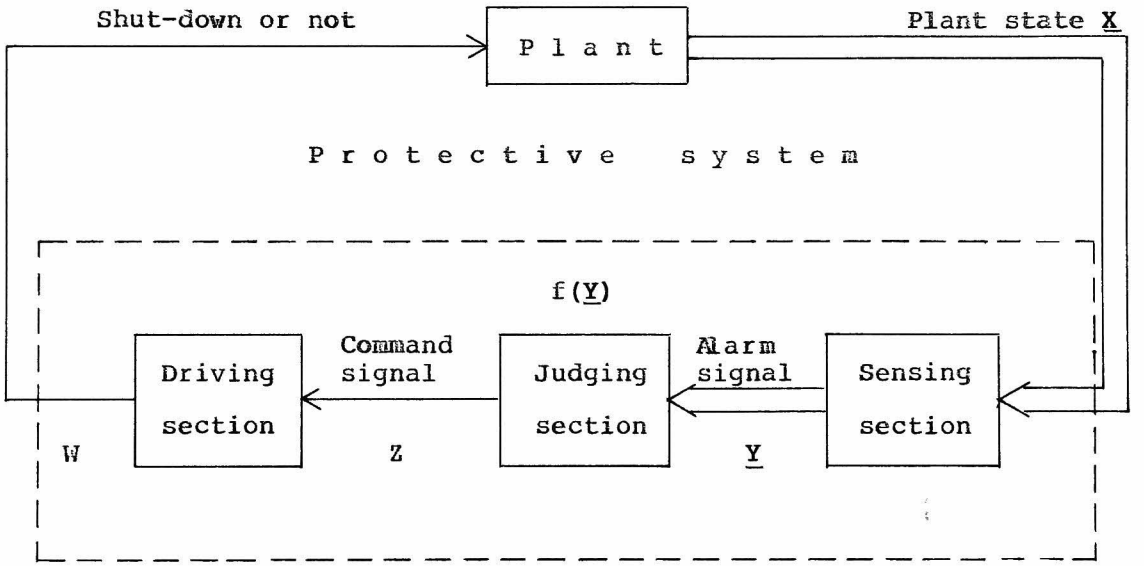

Fig. 8.1 Overall protective system structure

expression to implement the logic is also obtained. The evaluation of FD and FS probabilities of the judging and driving sections are shown in section 8.3.2.

8.2 PROBLEM STATEMENT

8.2.1 Assumptions

1 The protective system consists of a sensing, a judging, and a driving section.

2 The plant to be protected has N states.

3 Each plant state is either normal or abnormal.

4 Plant state i is monitored by N_i sensors of type i.

5 Each sensor is generating the sensor alarm or not.

6 The judging section is either issuing a command signal or not.

7 The driving section is either shutting down the plant or not.

8 Each section fails s-independently.

8.2.2 Notation

X_i binary indicator variable for plant state i

$$X_i = \begin{cases} 1, & \text{if plant state i is abnormal,} \\ 0, & \text{otherwise.} \end{cases}$$

$\underline{X}$ plant state vector: $(X_1,\ldots,X_N)$

Y_{ij} binary indicator variable for sensor j of type i

$$Y_{ij} = \begin{cases} 1, & \text{if sensor j of type i is generating the sensor alarm,} \\ 0, & \text{otherwise.} \end{cases}$$

$\bar{Y}_{ij}$ negation of Y_{ij}; $= 1 - Y_{ij}$

$\underline{Y}$ $(Y_{11},\ldots,Y_{1N_1},\ldots,Y_{N1},\ldots,Y_{NN_N})$

$f(\underline{Y})$ shut-down logic

$f(\underline{Y}) = \begin{cases} 1, & \text{if the judging section issues a command signal to shut down the plant.} \\ 0, & \text{otherwise.} \end{cases}$

Z binary indicator variable for the judging section

$Z = \begin{cases} 1, & \text{if the judging section is issuing a command signal,} \\ 0, & \text{otherwise.} \end{cases}$

W binary indicator variable for the driving section

$W = \begin{cases} 1, & \text{if the driving section is shutting down the plant,} \\ 0, & \text{otherwise.} \end{cases}$

a conditional FD probability of the judging section: $\Pr\{Z=0 \mid f(\underline{Y})=1\}$

b conditional FS probability of the judging section: $\Pr\{Z=1 \mid f(\underline{Y})=0\}$

c conditional FD probability of the driving section: $\Pr\{W=0 \mid Z=1\}$

d conditional FS probability of the driving section: $\Pr\{W=1 \mid Z=0\}$

$C_1(\underline{X})$ FD loss: loss caused when the driving section is not shutting down the plant under plant state $\underline{X}$

$C_2(\underline{X})$ FS loss: loss caused when the driving section is shutting down the plant under plant state $\underline{X}$

I_S s-expected total loss for a given shut-down logic $f(\underline{Y})$

The problem is to determine the optimal shut-down logic that minimizes an s-expected total loss caused by failures of the protective system.

8.3 PROBLEM SOLUTION

8.3.1 Optimal Shut-Down Logic

The s-expected total loss I_S caused by failures of the protective system is:

$$I_S = \sum_{\underline{X}} \sum_{\underline{Y}} \sum_{Z} \sum_{W} \{C_1(\underline{X})(1-W)+C_2(\underline{X})W\}\Pr\{W,Z,\underline{Y},\underline{X}\}. \quad (1)$$

The term $C_1(\underline{X})(1-W)$ indicates the FD loss, while $C_2(\underline{X})W$ indicates the FS loss. The probability $\Pr\{W,Z,\underline{Y},\underline{X}\}$ is expressed by the decomposition rule: $\Pr\{A\} = \Pr\{AB\} + \Pr\{A\bar{B}\}$, the production rule: $\Pr\{AB\} = \Pr\{A|B\}\Pr\{B\}$, and assumption 8, as follows:

$$\Pr\{W,Z,\underline{Y},\underline{X}\} = \sum_{f(\underline{Y})} \Pr\{W,Z,f(\underline{Y}),\underline{Y},\underline{X}\}$$

$$= \sum_{f(\underline{Y})} \Pr\{W|Z\}\Pr\{Z|f(\underline{Y})\}\Pr\{f(\underline{Y})|\underline{Y}\}\Pr\{\underline{Y}|\underline{X}\}\Pr\{\underline{X}\}.$$

The probability $\Pr\{f(\underline{Y})|\underline{Y}\}$ is deterministic, i.e., $\Pr\{f(\underline{Y})=1|\underline{Y}\} = f(\underline{Y})$. Then,

$$\Pr\{W,Z,\underline{Y},\underline{X}\} = \Pr\{W|Z\}\Pr\{Z|f(\underline{Y})=1\}\Pr\{\underline{Y}|\underline{X}\}\Pr\{\underline{X}\}f(\underline{Y})$$
$$+ \Pr\{W|Z\}\Pr\{Z|f(\underline{Y})=0\}\Pr\{\underline{Y}|\underline{X}\}\Pr\{\underline{X}\}\{1-f(\underline{Y})\}. \quad (2)$$

By eq. (2), I_S can be expressed as:

$$\begin{aligned} I_S = \sum_{\underline{X}} \sum_{\underline{Y}} \Big(& C_1(\underline{X})\big[\Pr\{W=0|Z=1\}\Pr\{Z=1|f(\underline{Y})=1\}f(\underline{Y}) \\ & + \Pr\{W=0|Z=1\}\Pr\{Z=1|f(\underline{Y})=0\}\{1-f(\underline{Y})\} \\ & + \Pr\{W=0|Z=0\}\Pr\{Z=0|f(\underline{Y})=1\}f(\underline{Y}\} \\ & + \Pr\{W=0|Z=0\}\Pr\{Z=0|f(\underline{Y})=0\}\{1-f(\underline{Y})\}\big] \\ & + C_2(\underline{X})\big[\Pr\{W=1|Z=1\}\Pr\{Z=1|f(\underline{Y})=1\}f(\underline{Y}) \\ & + \Pr\{W=1|Z=1\}\Pr\{Z=1|f(\underline{Y})=0\}\{1-f(\underline{Y})\} \\ & + \Pr\{W=1|Z=0\}\Pr\{Z=0|f(\underline{Y})=1\}f(\underline{Y}) \\ & + \Pr\{W=1|Z=0\}\Pr\{Z=0|f(\underline{Y})=0\}\{1-f(\underline{Y})\}\big] \Big) \\ & \times \Pr\{\underline{Y}|\underline{X}\}\Pr\{\underline{X}\}. \end{aligned} \quad (3)$$

Substitute $a = \Pr\{Z=0|f(\underline{Y})=1\}$, $b = \Pr\{Z=1|f(\underline{Y})=0\}$. $c =$

$\Pr\{W=0|Z=1\}$, and $d = \Pr\{W=1|Z=0\}$ into eq. (3), and we have I_S written as:

$$I_S = \sum_{\underline{X}} [\ C_1(\underline{X})+\{C_2(\underline{X})-C_1(\underline{X})\}(b+d-bc-bd)\ ]\Pr\{\underline{X}\}$$

$$- \sum_{\underline{X}} \sum_{\underline{Y}} (1-a-b)(1-c-d)\{C_1(\underline{X})-C_2(\underline{X})\}\Pr\{\underline{Y}|\underline{X}\}\Pr\{\underline{X}\}f(\underline{Y}). \qquad (4)$$

Define the function $GO(\underline{Y})$ as

$$GO(\underline{Y}) = (1-a-b)(1-c-d) \sum_{\underline{X}} \{C_1(\underline{X})-C_2(\underline{X})\}\Pr\{\underline{Y}|\underline{X}\}\Pr\{\underline{X}\}. \qquad (5)$$

Then,

$$I_S = \sum_{\underline{X}} [\ C_1(\underline{X})+\{C_2(\underline{X})-C_1(\underline{X})\}(b+d-bc-bd)\ ]\Pr\{\underline{X}\} - \sum_{\underline{Y}} GO(\underline{Y})f(\underline{Y}). \qquad (6)$$

The first summation on the right hand side of eq. (6) is independent of the logic $f(\underline{Y})$. Thus, I_S attains its minimum if we set $f(\underline{Y}) = 1$ for any $\underline{Y}$ satisfying $GO(\underline{Y}) > 0$. The optimal logic $f^*(\underline{Y})$ is:

$$f^*(\underline{Y}) = \begin{cases} 1, & \text{if } GO(\underline{Y}) > 0, \\ 0, & \text{otherwise.} \end{cases} \qquad (7)$$

We call $GO(\underline{Y})$ the switching function of the optimal shut-down logic $f^*(\underline{Y})$. This logic $f^*(\underline{Y})$ is optimal among all the Boolean logic structures.

The judging and driving section are reasonably reliable in practical applications. The inequality, $(1-a-b)(1-c-d) > 0$, holds. Then, the switching function $GO(\underline{Y})$ becomes equivalent to the switching function to determine the structure function in CHAPTER 7; the optimal shut-down logic is determined by the reliability of the sensing section. Thus, the results in CHAPTERS 5, 6, and 7 apply to the design of the shut-down logic.

The optimal shut-down logic $f^*(\underline{Y})$ can be implemented by the following Boolean function:

$$f^*(\underline{Y}) = \sum_{\underline{P}\in S} \{ \prod_{i=1}^{N} (\prod_{j=1}^{N_i} Y_{ij}(P_{ij})) \}, \tag{8}$$

where

$$S = \{ \underline{Y} \mid GO(\underline{Y}) > 0 \} : \text{set of path vectors of } f^*(\underline{Y}), \tag{9}$$

$$Y_{ij}(P_{ij}) = \begin{cases} Y_{ij}, & \text{if } P_{ij} = 1, \\ \bar{Y}_{ij}, & \text{otherwise.} \end{cases} \tag{10}$$

The sum of product expression, eq. (8), can be simplified by a Prime implicant algorithm [K19].

8.3.2 FD and FS Probabilities of Judging and Driving Sections

The FD and FS failure probabilities of the judging and driving sections can be similarly evaluated to those of the safety monitoring system. Clearly from Fig. 8.1, we make the following assumptions on these two subsystems:

(J-1) The components of the judging section get the same input signal from the sensing section.

(J-2) The judging section is composed of m components.

(D-1) The components of the driving section get the same command signal from the judging section.

(D-2) The driving section is composed of k components.

For example, a component of the judging section is a microcomputer processing instrumentation signals, and a component of the driving section is a shut-down valve.

Consider the judging section first. Let Z_i denote the state of component i:

$$Z_i = \begin{cases} 1, & \text{if component i is issuing a command signal,} \\ 0, & \text{otherwise.} \end{cases}$$

The state of the section is completely determined by $\underline{Z}$ =

$\{Z_1,\ldots,Z_m\}$:

$$Z = f_J(\underline{Z}). \tag{11}$$

The function $f_J(\underline{Z})$ is called the structure function of the judging section, representing how the judging section generates a command signal based on the state of its components.

If the components fail s-independently, the FD and FS probabilities, a and b, are calculated by the reliability function $h_J(\mathbf{Z})$ of the judging section in the same way as the safety monitoring system:

$$a = 1 - h_J(\underline{1-a}), \tag{12}$$

$$b = h_J(\underline{b}), \tag{13}$$

where

a_i : FD failure probability of component i:
$\Pr\{Z_i=0 \mid f(\mathbf{Y})=1\}$,

b_i : FS failure probability of component i:
$\Pr\{Z_i=1 \mid f(\mathbf{Y})=0\}$,

$\underline{1-a}$: $(1-a_1,\ldots,1-a_m)$,

$\underline{b}$: $(b_1,\ldots,b_m)$.

The same development follows in case of the driving section. The indicator variable for component i is defined by

$$W = \begin{cases} 1, & \text{if component i is shutting down the plant,} \\ 0, & \text{otherwise.} \end{cases}$$

The state of the driving section is denoted by the structure function $f_D(\underline{W})$:

$$W = f_D(\underline{W}), \tag{14}$$

where $\underline{W} = (W_1,\ldots,W_k)$.

The reliability function $h_D(\underline{W})$ expresses both FD and FS probabilities as follows in the case where failures of the

components are s-independent:

$$c = 1 - h_D(\underline{1-c}), \tag{15}$$

$$d = h_D(\underline{d}), \tag{16}$$

where

c_i : FD failure probability of component i:
$\Pr\{W_i=0 \mid Z=1\}$,

d_i : FS failure probability of component i:
$\Pr\{W_i=1 \mid Z=0\}$,

$\underline{1-c}$: $(1-c_1,\ldots,1-c_k)$,

$\underline{d}$: $(d_1,\ldots,d_k)$

If failures of the components are not s-independent, probabilities a, b, c, and d can be evaluated by the structure functions $f_J(\underline{Z})$ and $f_D(\underline{W})$, using Markov models (for example, see [D1]).

CHAPTER 9

CONCLUSION AND RECOMMENDATION FOR FURTHER RESEARCH

We developed the optimal logic structure of the safety monitoring system, in the sense it minimizes an expected total loss caused by the fail-dangerous (FD) and failed-safe (FS) failures of the safety monitoring system. The dissertation was roughly divided into three parts.

The first part, consisting of CHAPTERS 3 and 4, considered the safety monitoring system composed of several channels. Each of them consists of identical sensors and supervises a specific state of the plant. The problem is to obtain the optimal coherent structure for each channel. The optimal one-channel structure is proven to be k*-out-of-n:G structure in CHAPTER 3 and a simple formula to find optimal k* is given. The monotone trends of k* with respect to the failure probability of the plant, the FD and FS losses, are also shown. CHAPTER 4 dealt with multi-channel systems. The optimal logic structure for each channel is proven to be k-out-of-n:G structure, and then the problem is formulated into a non-linear integer programming (NLIP) problem. The NLIP problem can be solved by the extended Lawler and Bell's method throough a coordinate transformation.

The second part, CHAPTERS 5, 6, and 7, dealt with the safety monitoring system composed of sensors of different types. An

appropriate protective procedure is activated on the basis of the output of the sensors. The problem is how to obtain the optimal Boolean structure to combine the sensors. A simple rule to determine the optimal structure is given by a switching function. CHAPTER 5 considered the case where all the sensors monitor a specific plant state. The monotone property of the optimal structure with respect to the sensor shown in this chapter gives a systematic search method to determine it. Analytic solutions are also given for the case where all the sensors are identical. CHAPTER 6 studied the case where the system supervises several plant states. The similar switching function as in CHAPTER 5 is obtained, and the same development follows. CHAPTER 7 extended the results of CHAPTERS 5 and 6 into the case where failures of plant states are s-dependent. A classification of sensors into two classes, "positively reliable" and "negatively reliable", is proposed. The monotone property of the optimal structure with respect to the sensor is shown to depend on its reliability.

The last part, CHAPTER 8, discussed the optimal shut-down logic of the overall protective system, which is composed of driving, judging, and sensing sections. Each section fails in two ways: FD and FS. The optimal shut-down logic is obtained by a switching function. For the system with reliable judging and driving sections, the switching function becomes equivalent to that of CHAPTER 7. This means that the results of CHAPTER 5, 6, and 7 may apply to the design of the shut-down logic.

The topic recommended for further research is a dynamic logic structure. We dealt with a kind of dynamic logic: the probabilistic logic in [K9] where the structure is randomly

changing independent of the plant state. However, what we recommend now is another kind of dynamic logic structure, where the logic is changing on the basis of the monitored data. The development in this dissertation is a static optimization at a given time from this point of view, not considering the history of the data. The safety monitoring system is usually supervising its environment continuously with time. Then, the previous data monitored by the sensors are available not only for predicting the future phenomena of the plant, but also for detecting the failure of sensors. The logic should be changeable so that the output of the sensor estimated to be either FS or FD can be excluded. Such a dynamic logic can be implemented through the use of microcomputers. The problem is how to change the logic structure, depending on the history of monitored data. This study may be applied to the problem to change the shut-down logic in case of an inspection or maintenance of sensors.

REFERENCES

* The reference with an asterisk is the work of the author.

[A1] J. Ansell, A. Bendell, "On the optimality of k-ou-of-n:G systems", IEEE Trans. Reliability, Vol R-31, No. 2, Jun 1982, pp 206-210.

[B1] R.E. Barlow, L.C. Hunter, "Criteria for determining optimum redundancy", IRE Trans. Reliability and Quality Control, No. 9, Apr 1960, pp 73-77.

[B2] R.E. Barlow, L.C. Hunter, F. Proschan, "Optimum redundancy when components are subject to two kinds of failure", J. Soc. Indust. Appl. Math., Vol 11, No. 1, Mar 1963, pp 64-73.

[B3] R.E. Barlow, F. Proschan, Mathematical Theory of Reliability, John Wiley & Sons, Inc., New York, 1965, pp 185-195.

[B4] R.E. Barlow, F. Proschan, Statistical Theory of Reliability and Life Testing, Holt, Rinehart and Winston, New York, 1975, pp 1-51.

[B5] Y. Ben-Dov, "Optimal reliability design of k-out-of-n systems subject to two kinds of failure", J. Op. Res. Soc., Vol 31, 1980, pp 743-748.

[B6] Z.W. Birnbaum, J.D. Esary, S.C. Saunders, "Multi-component systems and structures and their reliability", Technometrics, Vol 3, Feb 1961, pp 55-77.

[B7] L.E. Booth, "Power plant econometric reliability : on

redundant tripping logic", IEEE Trans. Power Appratus and Systems, Vol PAS-100, No. 5. May 1981, pp 2512-2518.

[C1] S.C. Chay, M. Mazumder, "Determination of test intervals in certain repairable standby protective systems", IEEE Trans. Reliability, Vol R-24, No. 3, Aug 1975, pp 201-205.

[C2] C.J. Creveling, "Incresing the reliability of electronic equipment by the use of redundant circuits", Proceedings of the IRE, Vol 44, Apr 1956, pp 509-515.

[D1] B.S. Dhillon, C. Singh, Engineering Reliability, John Wiley & Sons, Inc., New York, 1981, pp 177-215.

[G1] K. Gopal, K.K. Aggarwal, J.S. Gupta, "Reliability optimizaton in systems with many failure modes", Microelectronics and Reliability, Vol 18, 1978, pp 423-425.

[G2] R. Gordon, "Optimum component redundancy for maximum system reliability", Operations Research, Vol 5, Apr-May 1957, pp 229-243.

[H1] F. Harbert, "The logic of emergency shut-down systems" Process Engineering, Dec 1977, pp 44-45.

[H2] C. Henin, "Double failure and other related problems in standby redundancy", IEEE Trans. Reliability, Vol R-21, No. 1, Feb 1972, pp 35-40.

[H3] K. Hyun, "Reliability optimization by 0-1 programming for a system with several failure modes", IEEE Trans. Reliability, Vol R-24, No. 3, Aug 1975, pp 206-210.

[I1] T. Inagaki, K. Inoue, H. Akashi, "Improvement of supervision schedules for protective systems", IEEE Trans. Reliability, Vol R-28, No. 3, Jun 1979, pp 141-144.

[I2]* K. Inoue, T. Kohda, H. Kumamoto, "Fault tree analysis of

sensor systems with two failure modes", Journal of Japan Society for Safety Engineering (in Japanese), Vol 19, No. 5, Oct 1980, pp 272-278.

[I3]* K. Inoue, T. Kohda, H. Kumamoto, I. Takami, "Optimal structures of sensor systems with two failure modes", IEEE Trans. Reliability, Vol R-31, No. 1, Apr 1982, pp 119-120.

[I4]* K. Inoue, T. Kohda, H. Kumamoto, I. Takami, "Optimal logical structure of multichannel safety monitoring systems", Trans. SICE (in Japanese), Vol 18, No. 6, Jun 1982, pp 635-640.

[J1] D.C. James, A.H. Kent Jr., J.A. Holloway, "Redundancy and the detection of first failures", IRE Trans. Reliability and Quality Control, Vol 11, Oct 1962, pp 8-28.

[K1] A. Kaufmann, D. Groucho, R. Cruon, Mathematical Models for the Study of the Reliability of Systems, Academic Press, New York, 1977, pp 190-206.

[K2] C. Kawaguchi, T. Itō, "Safety and reliability of reactor instrumentation", Nuclear Engineering (in Japanese), Vol 13, No. 9, Sep 1967, pp 49-56.

[K3] Y. Kimura, K. Hasegawa, A. Sekiguchi, "Microprocessor-based system for processing redundant instrumentation signals", IEEE Trans. Industrial Electronics and Control Instrumentation, Vol IECI-27, No. 3, Aug 1980, pp 218-222.

[K4]* T. Kohda, K. Inoue, H. Kumamoto, I. Takami, "Optimal logical structure of safety monitoring systems with two failure modes", Trans. SICE (in Japanese), Vol 17, No. 9, Dec 1981, pp 908-913.

[K5]* T. Kohda, H. Kumamoto, K. Inoue, I. Takami, "Optimal

structure of sensor systems composed of nonidentical sensors", Microelectronics and Reliability, Vol 32, No. 3, 1982, pp 445-456.

[K6]* T. Kohda, K. Inoue, H. Kumamoto, I. Takami, "Optimal logical structure of safety monitoring systems composed of sensors of different types", Proceedings of EUROCON '82 (Reliability in Electrical and Electronic Components and Systems, Ed. by E. Lauger and J. Møltoft), North-Holland Publishing Company, Amsterdam, 1982, pp 446-450.

[K7]* T. Kohda, H. Kumamoto, K. Inoue, "On optimization of protective system", Reports of Professional Group on Reliability of IECE (in Japanese), Vol R82-27, Oct 1982, pp 25-30.

[K8]* T. Kohda, H. Kumamoto, K. Inoue, "Optimal shut-down logic for protective systems", IEEE Trans. Reliability. Vol R-32, No. 1, Apr 1983.

[K9]* T. Kohda, H. Kumamoto, K. Inoue, "Optimization of probabilistic logic of safety monitoring systems", Trans. SICE (in Japanese), Vol 19, No. 4, Apr 1983.

[K10] P.J. Kolesar, "Linear programming and the reliability of multicomponent systems", Naval Reseach Logistics Quarterly, Vol 14, 1967, pp 317-328.

[K11] J.M. Kontoleon, "Optimum active-inactive times in supervised provective systems for nuclear reactors", Nuclear Science and Engineering, Vol 55, 1974, pp 216-224.

[K12] J.M. Kontoleon, "Optimum allocation of components in a special 2-port network", IEEE Trans. Reliability, Vol R-27, No. 2, Jum 1978, pp 112-115.

[K13] J.M. Kontoleon, "Analysis of a dynamic redundant system", IEEE Trans. Reliability, Vol R-27, No. 2, Jun 1978, pp 116-119.

[K14] J.M. Kontoleon, "Optimum supervision intervals and orders of supervision in nuclear protective systems", Nuclear Science and Engineering, Vol 66, 1978, pp 9-13.

[K15] J.M. Kontoleon, "Optimum trip level of m-out-of-n reactor temperature trip-amplifier sytems", IEEE Trans. Nuclear Science, Vol NS-26, No. 4, Aug 1978, pp 4645-4648.

[K16] J.M. Kontoleon, "Analysis of a dynamic redundant system with non-identical units", IEEE Trans. Reliability, Vol R-29, No. 1, Apr 1980, pp 77-78.

[K17] J.M. Kontoleon, "SAFE (nuclear reactor computer code)", Nuclear Science and Engineering, Vol 76, No. 1, Oct 1980, p 78.

[K18] J.M. Kontoleon, "Fail-to-safe and fail-to-danger analysis of logic protective networks", IEEE Trans. Reliability, Vol R-29, No.5, Dec 1980, pp 436-437.

[K19] H. Kumamoto, E.J. Henley, "Top-down algorithm for obtaining prime implicant sets of non-coherent fault trees", IEEE Trans. Reliability, Vol R-27, No. 4, Oct 1978, pp 242-249.

[K20] H. Kumamoto, E.J. Henley, "Protective system hazard analysis", Ind. Eng. Chem. Fundam., Vol 17, No. 4, 1978, pp 274-276.

[K21] H. Kumamoto, K. Inoue, E.J. Henley, "Computer-aided protective system hazard analysis", Computers and Chemical Engineering, Vol 5, 1981, pp 93-98.

[K22] H. Kumamoto, H. Ohtsuka, K. Inoue, "Expected number of

failure caused by protective systems", IEEE Trans. Reliability, Vol R-31, No. 2, Jun 1982, pp 219-221.

[L1] E.L. Lawler, M.D. Bell, "A method for solving optimization problems", Operations Research, Vol 13, Nov-Dec 1966, pp 1098-1112.

[L2] E.E. Lewis, Nuclear Power Reactor Safety, John Wiley & Sons, Inc., New York, 1977, pp 73-128.

[L3] J.P. Lipp, "Topology of switching element vs. reliability", IRE Trans. Reliability and Quality Control, No. PGRQC-10, Jun 1957, pp 21-34.

[M1] J.C.T. Mao, B.A. Wallingford, "An extension of Lawler and Bell's method of discrete optimization with examples from capital budgeting", Management Science, Vol 15, No. 2, Oct 1968, pp 51-60.

[M2] W.S. Meisel, "Reliability in digital systems with asymmetrical failure modes", IEEE Trans. Reliability, Vol R-18, No. 2, May 1969, pp 74-75.

[M3] H. Mine, K. Hatayama, "Reliability analysis and optimal redundancy for majority-voted logic circuits", IEEE Trans. Reliability, Vol R-30, No. 2, Jun 1981, pp 189-191.

[M4] K.B. Misra, T.S.M. Rao, "Reliability analysis of redundant networks using flow graphs", IEEE Trans. Reliability, Vol R-19, No. 1, Feb. 1970, pp 19-24.

[M5] E.F. Moore, C.E. Shannon, "Reliable circuits using less reliable relays", J. Franklin Inst., Vol 262, Sep 1956, pp 191-208; Vol 262, Oct 1956, pp 281-297.

[N1] Y. Nakagawa, Y. Hattori, "Reliability of all possible series-parallel redundant structures of m i.i.d. units with

two failure modes", IEEE Trans. Reliability, Vol R-29, No. 4, Oct 1980, pp 320-323.

[N2] Y. Nakagawa, Y. Hattori, "Discussion of "Optimization by integer programming of constrained reliability problems with several modes of failures"", IEEE Trans. Reliability, Vol R-30, No. 5, Dec 1981, pp 424-428.

[N3] T. Nakamura, "A new monitor and alarm system of gas leakage", Systems and Control (in Japanese), Vol 21, No. 7, Jul 1977, pp 376-384.

[N4] G.W.E. Nieuwhof, "A comparison study of the reliability of the two majority-vote instrumentation systems: two-of-three and three-of-four systems", Microelctronics and Reliability, Vol. 20, 1980, pp 13-24.

[O1] A.I. Ozkaynak, "The design of a solid state trip system for nuclear power plants", Microelectronics and Reliability, Vol 18, No. 3, 1978, pp 243-249.

[P1] M.J. Phillips, "The reliability of two terminal parallel-series networks subject to two kinds of failure", Microelectronics and Reliability, Vol 15, 1976, pp 535-549.

[P2] M.J. Phillips, "k-out-of-n:G systems are preferable", IEEE Trans. Reliability, Vol R-29, No. 2, Jun 1980, pp 166-169.

[P3] H.W. Price, "Reliability of parallel electrical components", IRE Trans. Reliability and Quality Control, Vol 9, Apr 1960, pp 35-39.

[S1] M. Sasaki, S. Kaburaki, S. Yanagi, "System availability and optimum spare units", IEEE Trans. Reliability, Vol R-26, No. 3, Aug 1977, pp 182-188.

[S2] B. Sayers, "Safety and risk in a chemical plant (a case

history)", 1979 Proceedings of Annual Reliability and Maintainability, Washington DC, 1979, pp 174-180.

[S3] M.L. Shooman, Probabilistic Reliability: An Engineering Approach, McGrow-Hill, New York, 1968, pp 293-323.

[S4] C. Singh, A.D. Patton, "Protective system reliability modeling: unreadiness probability and mean duration of undetected faults", IEEE Trans. Reliability, Vol R-29, No. 4, Oct 1980, pp 339-340.

[T1] I. Takami, T, Inagaki, E. Sakino, K. Inoue, "Optimal allocation of fault detector", IEEE Trans. Reliability, Vol R-27, No. 5, Dec 1978, pp 360-362.

[T2] I. Takami, K. Inoue, E. Sakino, H. Kumamoto, "Optimal reliability design of k-out-of-n systems", Proceedings of EUROCON '82 (Reliability in Electrical and Electronic Components and Systems, Ed. by E. Lauger and J. Møltoft), North-Holland Publishing Company, Amsterdam, 1982, pp 201-205.

[T3] F.A. Tillman, "Optimization by integer programming of constrained reliability problems with several modes of failure", IEEE Trans. Reliability, Vol R-18, No. 2, May 1969, pp 47-53.

[T4] S.N. Todd, "The use of microprocessors in gas-cooled nuclear reactor", Electronics and Power, Vol 27, No. 4, Apr 1981, pp 323-325.